Defense Manpower Data Center (DMDC) Contractor Verification System

User Training Guide

Version 1.7
September 2006

Prepared by:
DMDC-West
Card Technology and Identity Solutions Division

Document History

Version	Date	Author	Comments
0.1	12/18/02	IJO	Origin
1.0	1/31/03	IJO/WS	Revision
1.1	3/04/03	IJO/WS	Revision
1.2	5/09/03	IJO	Revision, incorporating Navy comments
1.3	8/6/03	IJO	Revision, incorporating comments by Wade Shaffer
1.4	9/23/04	IJO	Revision, reflecting upgrade
1.5	5/13/05	IJO	Revision, addition of e-mail Contractor reverification notification content. Addition of modified page for TA Change Contact Information page.
1.6	12/10/05	IJO	New Section 3 added
1.7	11/17/06	IJO	Revision incorporates changes made for version 2.0

TABLE OF CONTENTS

TABLE OF FIGURES

1   Document Overview

1.1   Purpose

The following training guide supports usage of the Contractor Verification System (CVS). CVS was designed in 2003 to replace DD Form 1172-2 paper "Application for Department of Defense (DoD) Common Access Card DEERS Enrollment"[1]. As a web-based system, CVS allows DoD contractors to apply for a Common Access Card (CAC) electronically via the internet. Government sponsors are responsible for approving the contractor applications to receive CACs.

1.2   Background

The DoD began issuing advanced identification (ID) cards for Active Duty Military, Selected Reserves, DoD Civilians, and "inside the wall" contractors in October 2000. The new Common Access Card (CAC) is a personalized smart card - a plastic card the size of a credit card with an embedded integrated circuit chip (ICC) for storing and processing data. Incorporated with Public Key Infrastructure (PKI) security, the CAC consolidates multiple credentials and data and may be used for a variety of applications, including network security and secure e-mail communication.

The current CAC features 32 kilobytes of Electronically Erasable Programmable Read Only Memory (EEPROM) and supports on-card secure cryptographic functions including key generation,[2] encryption and digital signing. The ICC contains protected data about the card holder (including Personal Identification Number [PIN]), personal demographics, benefits, digital certificates, and card management/security applets. Three unique x.509v3 1024 bit digital certificates stored on the chip allow the cardholder to digitally sign documents, encrypt data for transmission or storage, and establish secure Web sessions to access and update information via the Internet.

A new version of the CAC is equipped with 64 kilobytes of EEPROM. The increased memory will provide for the creation more complex and functional applets in support of business processes.

The Defense Manpower Data Center (DMDC) Card Technology and Identity Solutions (CT&IS) and Access Card Office (ACO) are the sponsoring organizations for the CAC program.

---

[1] Copy of the 1172-2 form and Instructions are attached as Appendix A and Appendix B respectively.

[2] Keys affect the way data is encrypted, only a correct key can decrypt the encrypted data. In the case of Public keys, data encrypted with the public key may be decrypted only with the private key.

2   CVS Roles and Responsibilites

2.1   Service Point of Contact Role and Responsibilities

The SPOC is appointed for CVS management and operation. The SPOC manages the CVS for their own Service/Agency. He/she coordinates with the Defense Manpower Data Center (DMDC) and establishes sites with CVS capability. The SPOC also oversees TASM registration, and provides any other required field support. SPOCs are responsible for meeting TA position requirements (specified in Section 10.1.1),

Specifically, the SPOC administers the CVS within their service/agency, including entering and updating Site Identification (site ID) numbers and Trusted Agent Security Managers (TASMs). He/she coordinates requests for new or additional CVS capability between service/agency and the DMDC. The SPOC works with the DMDC Security Team (DST) to register and/or remove site IDs and TASMs. He/she creates policies, operating procedures and other supporting documentation in support of the service/agency specific implementation.

2.2   Trusted Agent Security Manager Role and Responsibilities

TASM acts as a Trusted Agent who troubleshoots CVS questions/issues for their site, and manages all TA users for their site. He/she trains an alternate site TASM and all TAs operating CVS. He/she also provides visibility for the CVS program at their site via staff call, newsletter or website, or other effective means. Information, that he/she provides, should include the CVS location, hours of operation, telephone numbers, and other pertinent data. The TASM is also responsible for submitting requests via their SPOC for new or additional CVS capability. The TASM also coordinates all CVS matters with the SPOC. The TASM must notify the SPOC and DMDC Support Center of any CVS outage loss, or any suspected or known CVS system compromise. The TASM must also ensure positive identification for all Site TAs. TASMs are responsible for meeting TA position requirements (specified in Section 9.1.2).

The Service/Agency POC is responsible for appointing Trusted Agent Security Managers (TASMs). Defense Enrollment & Eligibility Reporting System (DEERS) must have a record for The Trusted Authority Security Manager (TASM) before he/she may register.

Before the TASM can create or manage Trusted Agent (TA) accounts, he/she must log into the Learning Module System (LMS) and gain certification to perform the tasks associated with the TASM role.

2.3   Trusted Agent Role and Responsibilities

The TA's primary role in the field is to sponsor a contractor to receive a CAC. Sponsoring a contractor is a multi-step process which includes establishing a contractor's

need for logical/physical access to either a DoD network or facility, verifying that the employer organization has vetted the contractor, and establishing the affiliation of the contractor with the service/agency. The contractor requesting a CAC is vetted by the employer organization using a DoD approved process. DoD civilians requesting a CAC are vetted by the OPM.

TAs are responsible for meeting TA position requirements (specified in Section 9.1.3).

The TA must also notify the TASM of site capability loss; TASM, SPOC, or DMDC Support Center of any suspected or known CVS system compromise; TASM of any malfunctions or anomalies with CVS. (TAs should contact the DMDC Support Center when the local TASM is unavailable).

Trusted Agents are required to gain certification to perform the tasks associated with the TA using the Learning Module System (LMS) before they can log into the CVS.

3 CVS Business Process Overview

3.1 Site Creation and TASM Registration

The Service/Agency POC will contact DEERS/RAPIDS Operations Support to establish a Site ID and have the TASMs added to the Site in the system. Once the SPOC notifies DEERS/RAPIDS Operations Support, DEERS/RAPIDS Operations Support typically takes 2 days to set up accounts for site ids and TASMs and another two days for FedEx delivery. The Service/Agency POC will transmit the data required for TASM registration to DEERS/RAPIDS Operations Support by digitally signed e-mail. DEERS/RAPIDS Operation Support will generate the TASM record in the DEERS security model. DEERS/RAPIDS Operations will then deliver new log in information to the TASM via FedEx or US Mail.

3.2 TA Registration

To register a Trusted Agent (TA) in CVS, the TASM must log into the DEERS Security Online Website. To register a TA the TASM uses the TA's Social Security Number (SSN). The TA must already have been enrolled in DEERS to be registered in CVS. A username and initial password is generated for the TA and mailed to TASM for distribution. The TA may login either by using the username/password he/she receives through mail or by using his/her CAC. TA registration provides access to the CVS system only.

3.3 Contractor Log In

When a contractor receives his/her User ID and temporary password from the TA he/she has 7 days to log in and begin the application process or the CVS will automatically

disable the contractor's account. Once the contractor has logged in for the first time, he/she has 30 days to complete the application process. The contractor will be able to save a partially completed application; however, the application will not be processed until it has been submitted in a complete form. Once a completed application is submitted, the system automatically notifies the TA. No further changes are allowed to be made to the application once it is submitted.

3.4 Entering Previously Issued/Existing CACs

Many contractors carry CACs that were issued prior to CVS implementation by their contracting government organization. CACs in this category do not need to be extended based on their end dates and should be sponsored by the TA using the CVS. A new CAC need not be issued to the contractor.

3.5 Verification and CAC Issuance

When the TA receives notification that the contractor application has been received, the TA will login to CVS using either his/her CAC or his/her username/password and review the application. The TA has 30 days to review the application from the time that the contractor submits the application. Upon review, the TA may approve the application, return the application to the contractor for corrections, or reject the application. Before approving an application, the TA must establish a contractor's need for logical/physical access to either a DoD network or facility, verify that the employer organization has vetted the contractor, and establish the affiliation of the contractor with the service/agency. The contractor requesting a CAC is vetted by the employer organization using a DoD approved process. DoD civilians requesting a CAC are vetted by the OPM.

In the event that the application is rejected, the system notifies the contractor and records the rejection. If the application is approved, the system will update DEERS with the contractor information and direct the contractor by e-mail to proceed to a RAPIDS workstation for CAC issuance.

Once the TA approves the application, the contractor has 90 days to obtain a CAC through RAPIDS.

3.6 Contractor reverification

Trusted agents are required to reverify contractors every six months (180 days). In addition to confirming the contractor's continued affiliation with the DoD, the TA must confirm the contractor's continued need for a CAC. The system obtains current TA e-mail address information from DEERS, and notifies TAs by e-mail of contractors who need to be reverified. When notice is received that a contractor must be reverified, the TA will log in to the system and review the contractor's records. During review, the TA may reverify or revoke the contractor records. Procedures for revoking contractor records are discussed below.

The schedule for e-mail notifications for contractors who need to be reverified is provided in Appendix C.

3.7 CAC Expiration

Common Access Cards typically are set to expire in three years. As the expiration date approaches, a contractor will need to contact their TA and apply for a new card.

Before the TA initiates the application process for a new CAC, he/she must verify that the contractor will need the card.

3.8 Contractor Revocation

The TA has the capability to revoke a contractor at any time. After logging into the system, the TA selects the contractor record. To process a revocation, the TA selects the revoke button. In addition to processing the request, the TA must provide a reason for the revocation. The system will update DEERS. DEERS will update the Certificate Authority (CA). The CA will subsequently revoke the contractor's certificates. The contractor receives notice of his revocation via e-mail. The TA should collect and return the CAC in accordance with standard procedures.

3.9 Trusted Agent Sponsorship Transfer

The TASM will be responsible for transferring contractor sponsorship between TAs. To initiate the transfer, the TASM will log into CVS and select the contractors to be transferred from the list of contractors assigned to a particular TA. After selecting the contractors, the TASM assigns them to a new TA. The system notifies both TA and affected contractors of the new assignments via e-mail.

4 Time Allowed to Complete Key CVS Procedures

Procedure	Actor	Description
First login	Contractor	Once a Trusted Agent creates an application, a contractor has 7 days to login to the CVS website and begin the application process.
Time to review	Contractor	After the contractor performs the initial log in, the contractor has up to 30 days to

application		complete application, providing the save button is selected before exiting the application. Note that once the contractor submits an application, he/she may no longer make changes to it unless it is returned for corrections by the TA.
Time to review application	Trusted Agent	Once a contractor submits an application, a Trusted Agent has 30 days to review it.
Time to have CAC issued	Contractor	Once a Trusted Agent approves an application, a contractor has 90 days to have CAC issued to him or her.
Time to reverify contractor account	Trusted Agent	Six (6) months after a Trusted Agent approves an application, he or she will need to reverify it, provided that the application has not been disabled or revoked in the interim. The system will send notification that the application must be reverified will be sent by email at 30, 20, and 10 day intervals before the due date.
Time to next reverify contractor account	Trusted Agent	After a Trusted Agent has reverified a contractor application, he or she will need to verify it again in 6 months.

5 Terminology

The terms "Top row navigation" and "Second row navigation" are used throughout this document to refer to the standard tabular arrangement of links between pages as depicted in Figure 1.
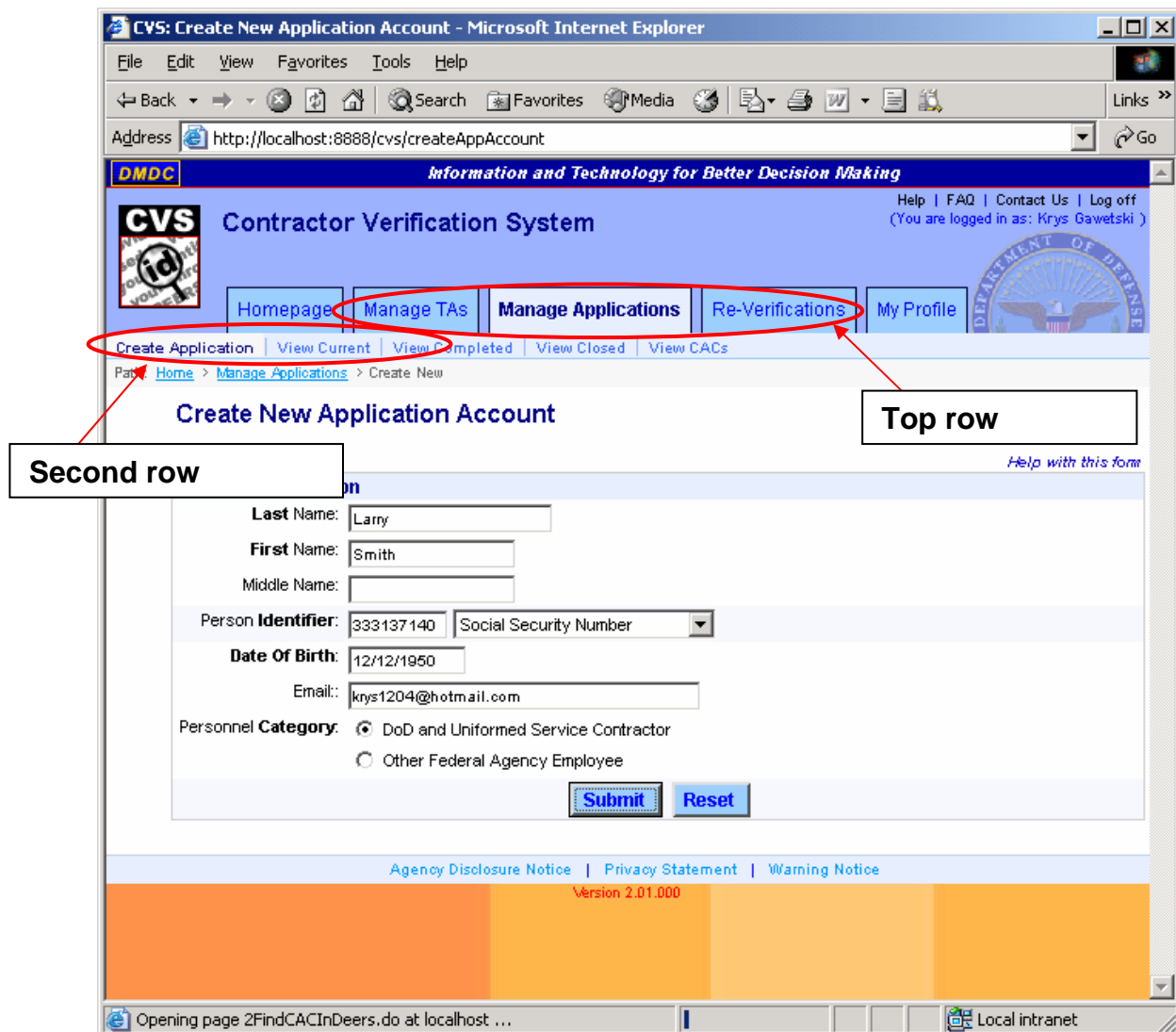
Figure 1 - Navigational layout

6 Common Screens

6.1 Outage Schedule

The CVS Outage Schedule, accessible from a link on the home page for TASM, TA, and Contractors, provides updated information regarding the availability of CVS web services.

Figure 2 - Outage Schedule

6.2 Learning Module System

Before using the CVS, the TASM and TA must gain certification to perform the necessary actions associated with his/her role through the Learning Module System (LMS).
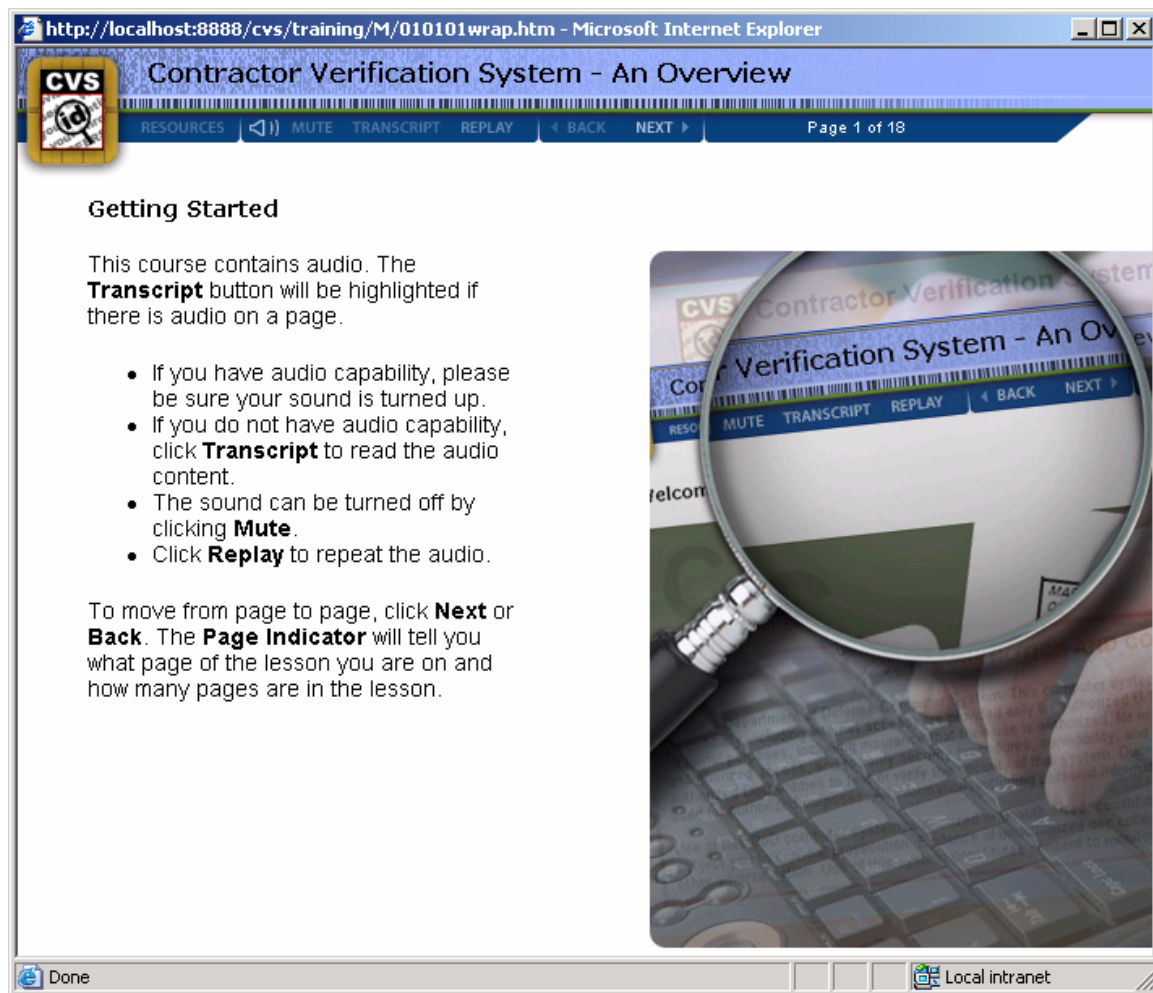
Figure 3 - Learning Module System

6.3   Frequently Asked Questions (FAQs)

The CVS Frequently Asked Questions page is accessible from every screen in the CVS web-site.

6.4   Contact

The CVS Contact screen is accessible from every screen in the CVS web-site.

6.5   User Guide (Online version)

A digital version of this User Guide is accessible from every screen in the CVS web-site.

7   TASM User Guide

7.1   Logging in

A TASM must gain certification to perform the tasks of a TASM from the Learning Module System before logging into the CVS.

1) Go to the CVS web site and **log in** using either your CAC or your User Name and password. DEERS/RAPIDS Operations delivers new log in information to newly appointed TASMs via FedEx and US Mail for APO and FPO addresses (see Section 3.1). CAC and User Name/password log in methods vary as follows:

Logging in with CAC:

If you choose to log in with your CAC, your card will need to be valid (i.e. your card and certificates have not expired). You will not be able to log in successfully if you do not have access to the CVS as it is established by the TASM using Security Online (see Section 7.2). At first log in, you will be directed to the "My Profile" page, where you will have the opportunity to update your user account information including email address. After the initial log in, you will be directed to the TA Homepage after successful log in. If your account has been suspended, you will receive notification on the log in page. Log in will fail if: an incorrect URL is entered, the application times out, the page you are on for an application is out-of-sync with the actual status of the application.

Logging in using User Name and password:

If you choose to log in using User Name and password as securely provided to you by the TASM for your site, you will not be able to log in successfully if you do not have access to the CVS as it is established by the TASM using Security Online (see Section 7.2). At first log in, you will be directed to the "My Profile" page, where you will have the opportunity to change your password and update your user account information including email address. After the initial log in, you will be directed to the "TA Homepage" after successful log in. If your account has been suspended, you will receive notification of the fact on the log in page. Log in will fail if: an incorrect URL is entered, the application times out, if the page you are on for an application is out-of-sync with the actual status of the application.

Figure 4 – CVS log in page

7.2   Creating a Trusted Agent

1) To register a Trusted Agent (TA) in CVS, the TASM must use the DEERS Security Online Website. To register a TA, the TASM uses the TA's Social Security Number (SSN). The TA must already have been enrolled in DEERS to be registered in CVS. DEERS/RAPIDS Operations Support generates username and initial password for the TA and the account information is sent FedEx (US mail for APO and FPO addresses) to the TASM for distribution. The preferred method of giving the TA his/her user account information is to hand the unopened mailed package to the TA directly.
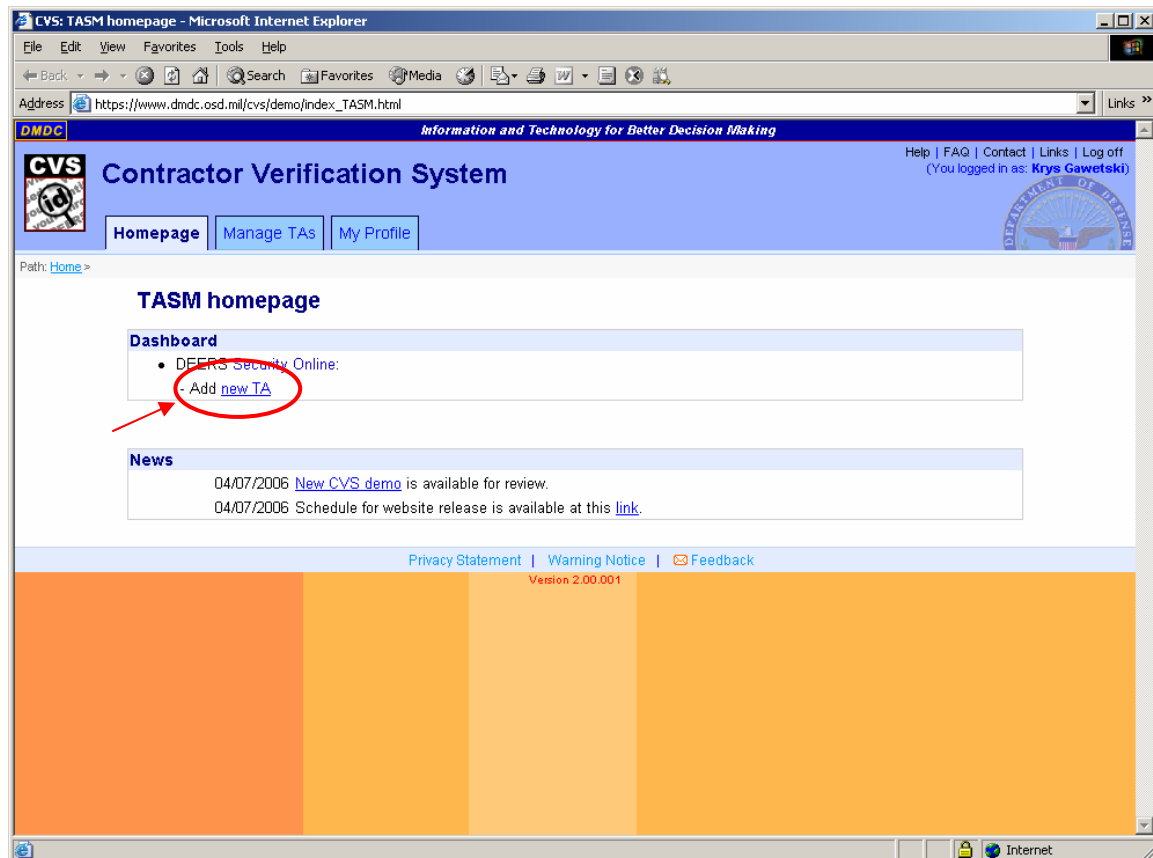
Figure 5 – TASM home page

2) To access the DEERS Security Online site from CVS, click the "Add new TA" link as shown in Figure 5 from the TASM home page. When the link to the DEERS Security Online site is selected, the home page for that site will open in a new browser window. Perform the necessary actions using that site. The Application ID (APP_ID) for the CVS is 229. Close the browser window after log out to secure all transactions. Questions pertaining to the usage DEERS Security Online site, including adding new site users, are addressed in the training document for the DEERS Security Online Website, "DEERS Online Security Training Manual."
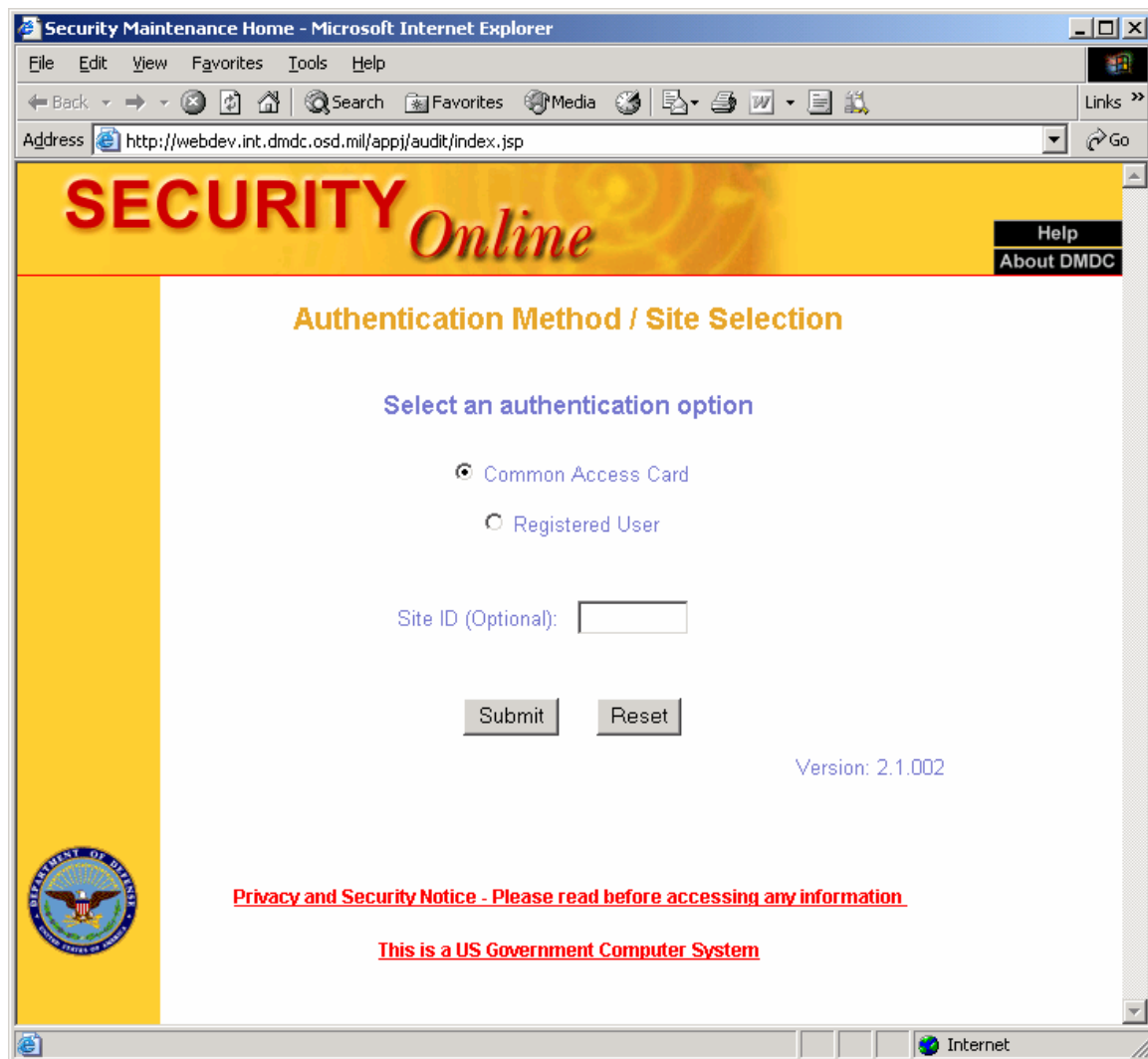
Figure 6 - Security Online home page

7.3 Managing TA accounts

1) Select the "Manage TAs" link from the top row navigation. The site will direct you to the "View Trusted Agents" page.

2) From the "View Trusted Agents" page, you may reassign a TA's contractors to another TA by clicking either the "CACs" link, which provides a list of contractors who possess a CAC, or the "Apps" link, which lists contractors who are applying for CACs, in the far right column. The CACs link will open up the "View CACs – reassign" page (see Section 7.3.1). The APPs link will open up the "View Applications – reassign" page (see Section 7.3.2). You may also email the TA by clicking on the TA's email link in the Email column.
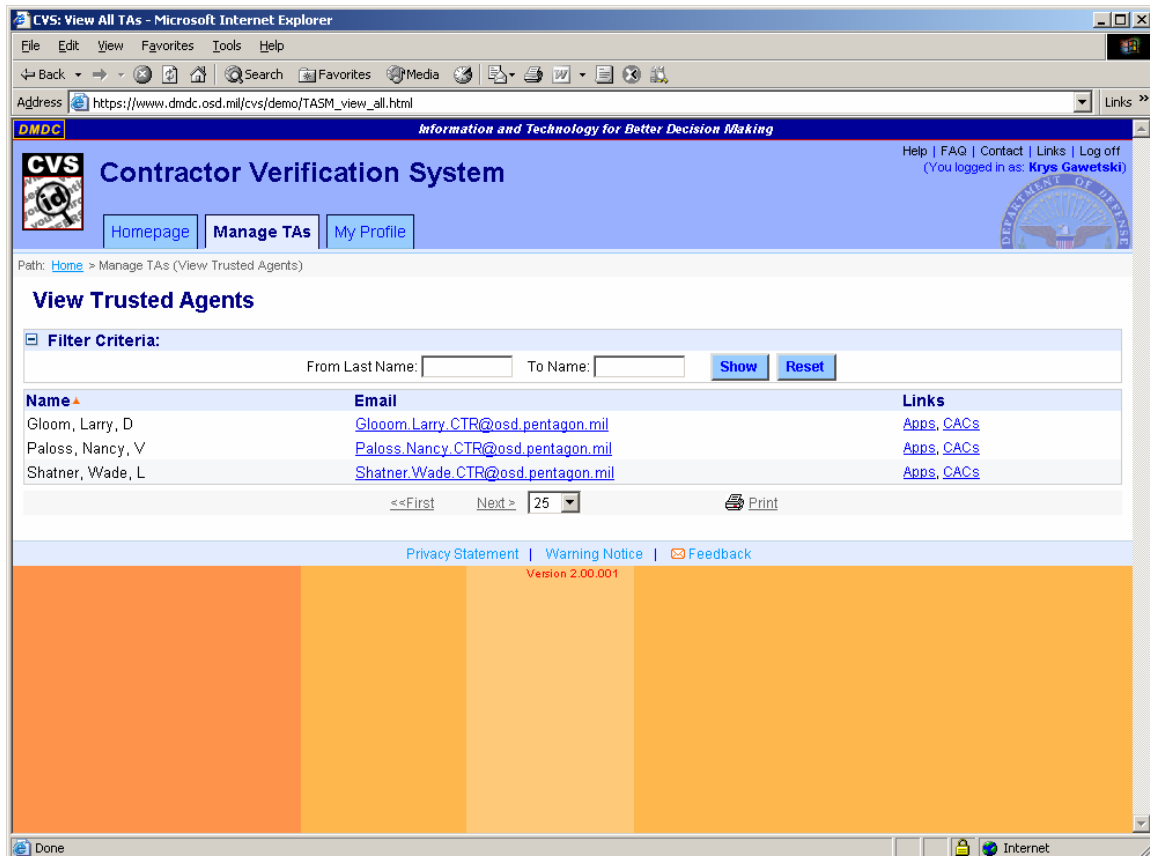
Figure 7 - View Trusted Agents

7.3.1   Reassigning CAC holders

1) When the "CACs" button has been selected, the system will display information for CAC holders assigned to the selected TA including login ID, home email, last access and status of application. Reassign contractors by selecting the check box next to the contractor name (see Figure 8, #1). Select a TA to be assigned the contractors checked in the check boxes from the drop-down list of TA names (see Figure 8, #2). You may re-assign more than one contractor at a time. Once the TA name is selected, click the button labeled "Reassign" (see Figure 8, #3). You may view the contractor's application by clicking on the contractor's name.
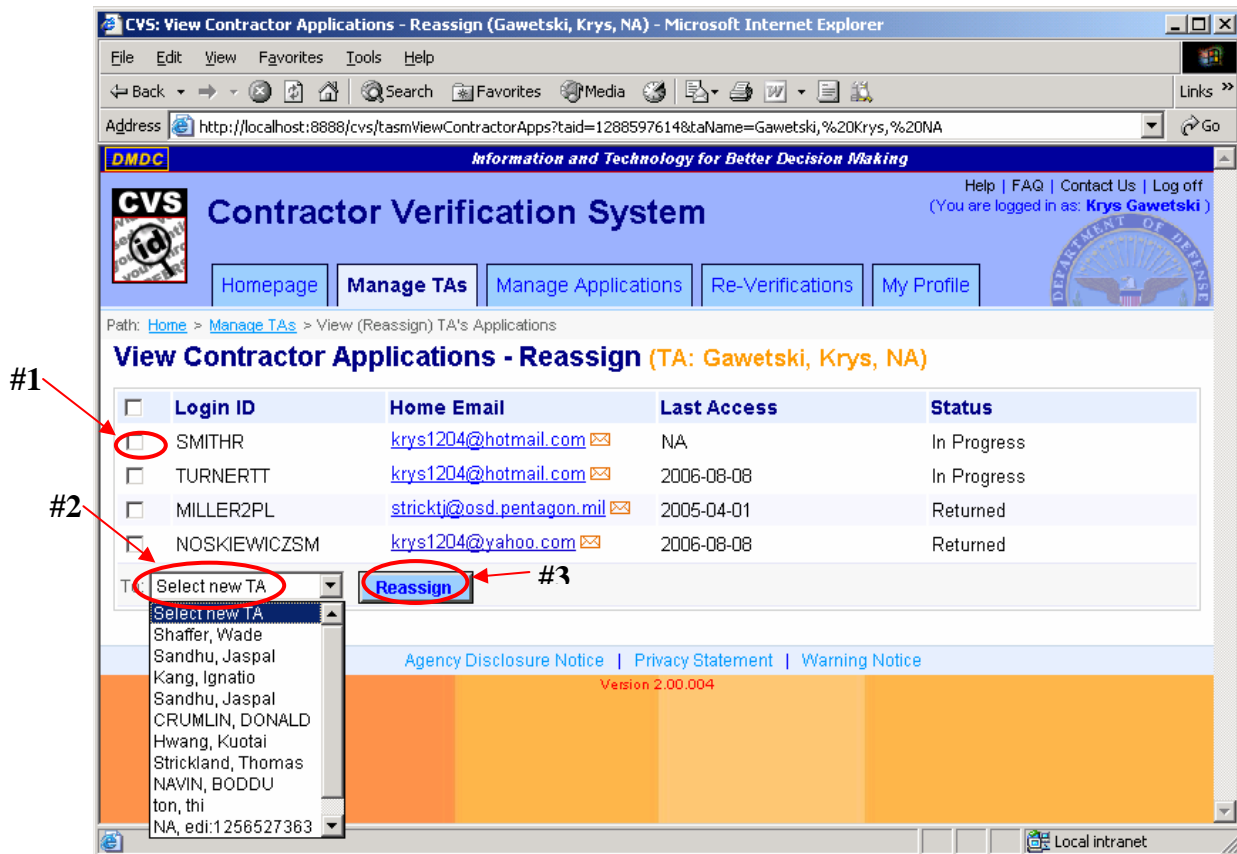
Figure 8 - View CACs - Reassign

7.3.2   Reassigning Applicants for CACs

1) When the "Apps" button has been selected, the system will display information for CAC applicants assigned to the selected TA including login ID, home email, last access and status of application. Reassign contractors by selecting the check box next to the contractor name (see Figure 9, #1). Select a TA to be assigned the contractor checked in the check boxes from the drop-down list of TA names (see Figure 9, #2). More than one contractor may be re-assigned at a time. Once the TA name is selected, click the button labeled "Reassign" (see Figure 9, #3). You may view the contractor's application by clicking on the contractor's name.
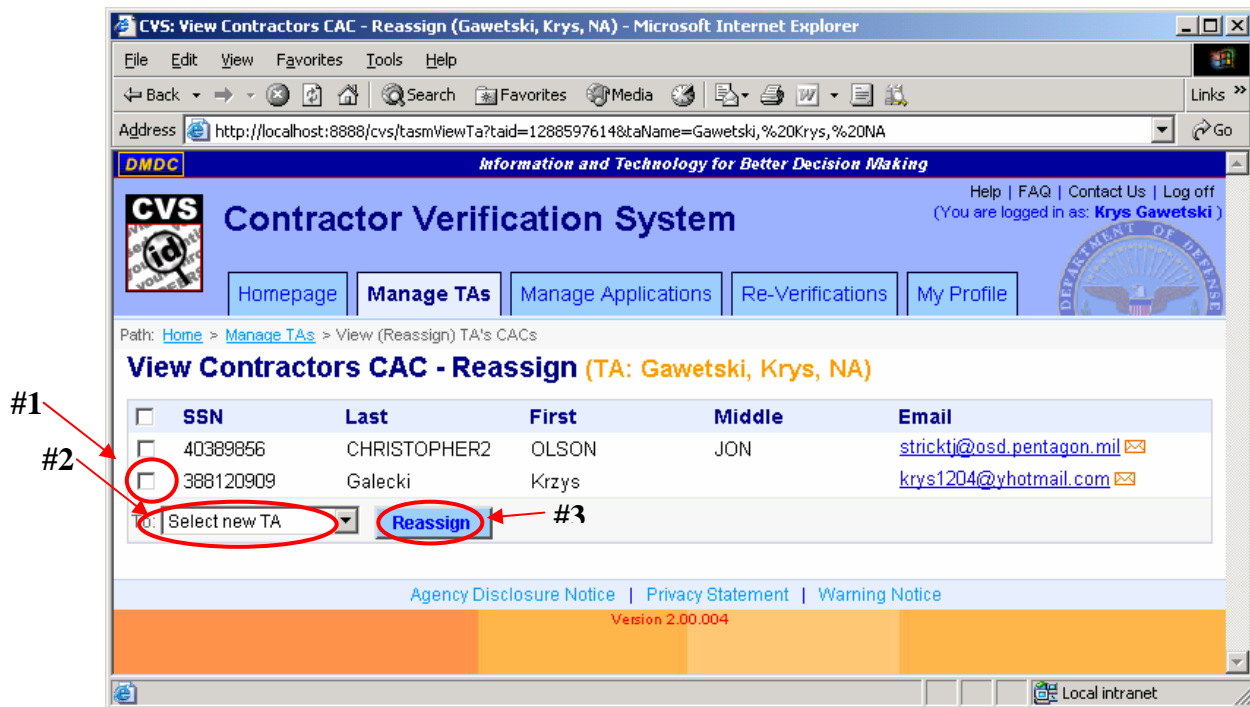
Figure 9 - View Applications - Reassign

2) When the reassignment is complete, the system will send an email to both the former assigned TA and the newly assigned TA. In addition to the email, the system will display a page confirming the success of the reassignment.

7.4   Changing a TASM User Profile (Contact Information and Password)

1) To update your account information, select the "My Profile" button from the top row navigation. The TA Edit Profile page will load and provide means to change contact information and password. Click the +/- toggle button to alternately hide or show either the contact or the password information and update form.

Figure 10 – TA Edit Profile page

2) To change contact information, enter and confirm your preferred new e-mail address, as well as your first, middle and last name. Click the "Save" button to submit the change.

3) To change your password, enter your old password and your preferred new password in the space provided. Re-enter your new password to confirm your selection. Follow the established password format: 8 characters, mixed case, one number, and one special character. Then, click on the "Change Password" button. If your password does not meet the specified requirements, the system will return an error message. The system will return this error message until the submitted password complies with the requirements.

4) The system will display a screen confirming the success of the password change request.

8 TA User Guide

8.1 TA log in

A TA must gain certification to perform the tasks of a TA from the Learning Module System before logging in to CVS.

1) Go to the CVS web site and **log in** using either your CAC or your User Name and password. CAC and User Name/password log in methods vary as follows:

Logging in with CAC:

If you choose to log in with your CAC, your card will need to be valid (i.e. your card and certificates have not expired). You will not be able to log in successfully if you do not have access to the CVS as it is established by the TASM using Security Online (see Section 7.2). At first log in, you will be directed to the "My Profile" page, where you will have the opportunity to update your user account information including email address. After the initial log in, you will be directed to the TA Homepage after successful log in. If your account has been suspended, you will receive notification on the log in page. Log in will fail if: an incorrect URL is entered, the application timeouts, the page you are on for an application is out-of-sync with the actual status of the application.

Logging in using User Name and password:

If you choose to log in using User Name and password as securely provided to you by the TASM for your site, note that you will not be able to log in successfully if you do not have access to the CVS as it is established by the TASM using Security Online (see Section 7.2). At first log in, you will be directed to the "My Profile" page, where you will have the opportunity to change your password and update your user account information including email address. After the initial log in, you will be directed to the "TA Homepage" after successful log in. If your account has been suspended, you will receive notification on the log in page. Log in will fail if: an incorrect URL is entered, the application timeouts, the page you are on for an application is out-of-sync with the actual status of the application.

Figure 11 - CVS log in page

2) The TA home page provides a dashboard that contains links and counts for applications according to different degrees of status. The home page also provides news regarding CVS operations. Using the links in the dashboard frame you may review applications, reverify applicants, view in-progress applications, view approved applications, and view returned applications.
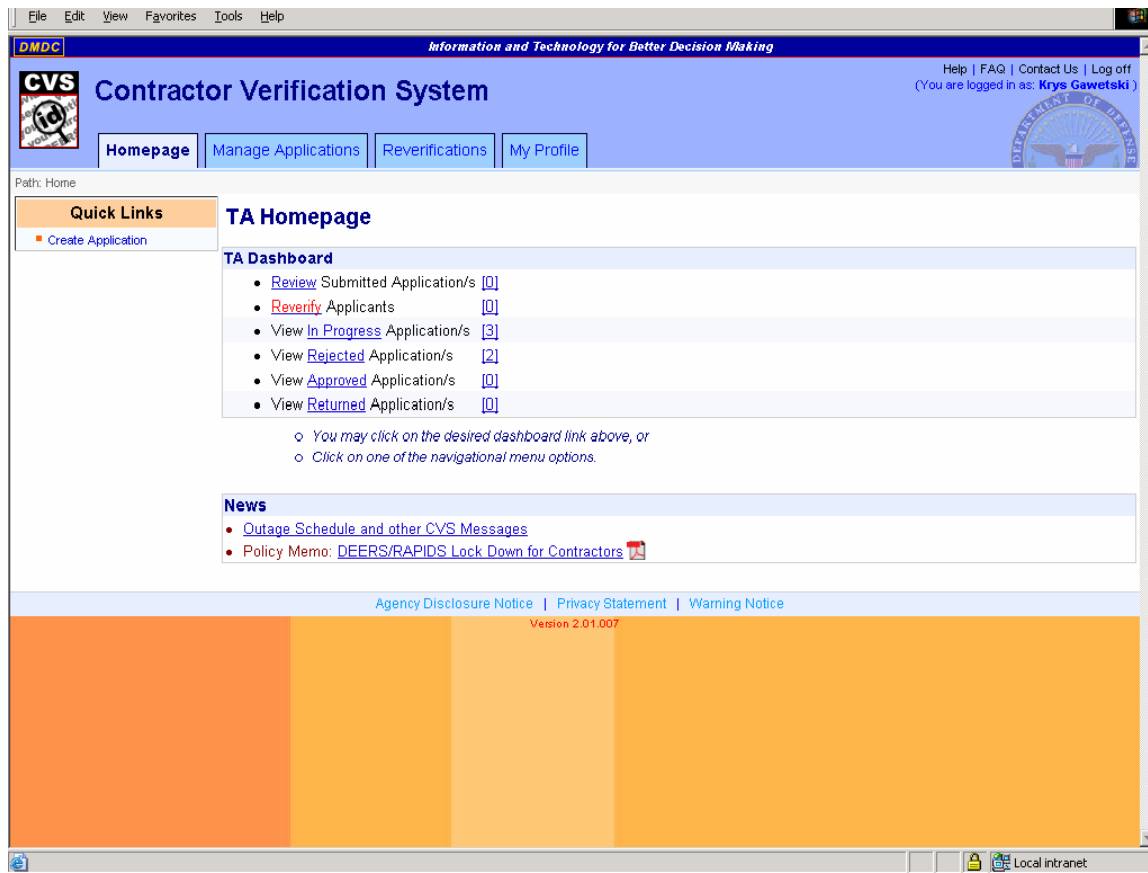
Figure 12 - TA home page

8.2   *Creating a New Application*

1) The "Create New Application Account" page will appear when the "Create Application" link is selected from the Quick Links box, or from the second row navigation under "Manage Applications".

Figure 13 - Create New Application page

2) Enter last name, first name, middle name (optional), cadency, person identifier (Social Security number, etc.), date of birth, email, and personnel category (DoD and Uniformed Service Contractor or Other Federal Agency Employee). Note that the fields that are marked with a cross ("†") cannot be changed by the contractor once the application is submitted.

Note that the fields that are marked with a cross ("†") cannot be changed by the contractor once the application is submitted.

3) When you have entered the information, the application will return a "Create New Application Account - Confirm" page that asks you to confirm whether the information for the applicant is new to the CAC issuance process.

Figure 14 - Create New Application Account Confirm

4) If the attempt to create a new account fails, you will see the "Create Account Failure" page (see Figure 15) which provides explanation for the failure, a Reset button to restart the process of creating a new account (see Figure 15, #1), and instructions to obtain further information.

Figure 15 - Create Account Failure

5) If the account is successfully created after confirmation, you will see the "Create New Application Account – Success" page with the contractor's login user ID and initial password. The page also provides information for the number of days that the contractor has to log into the CVS and to fill out (complete) and submit the application before the account is disabled (see Figure 16, #1).
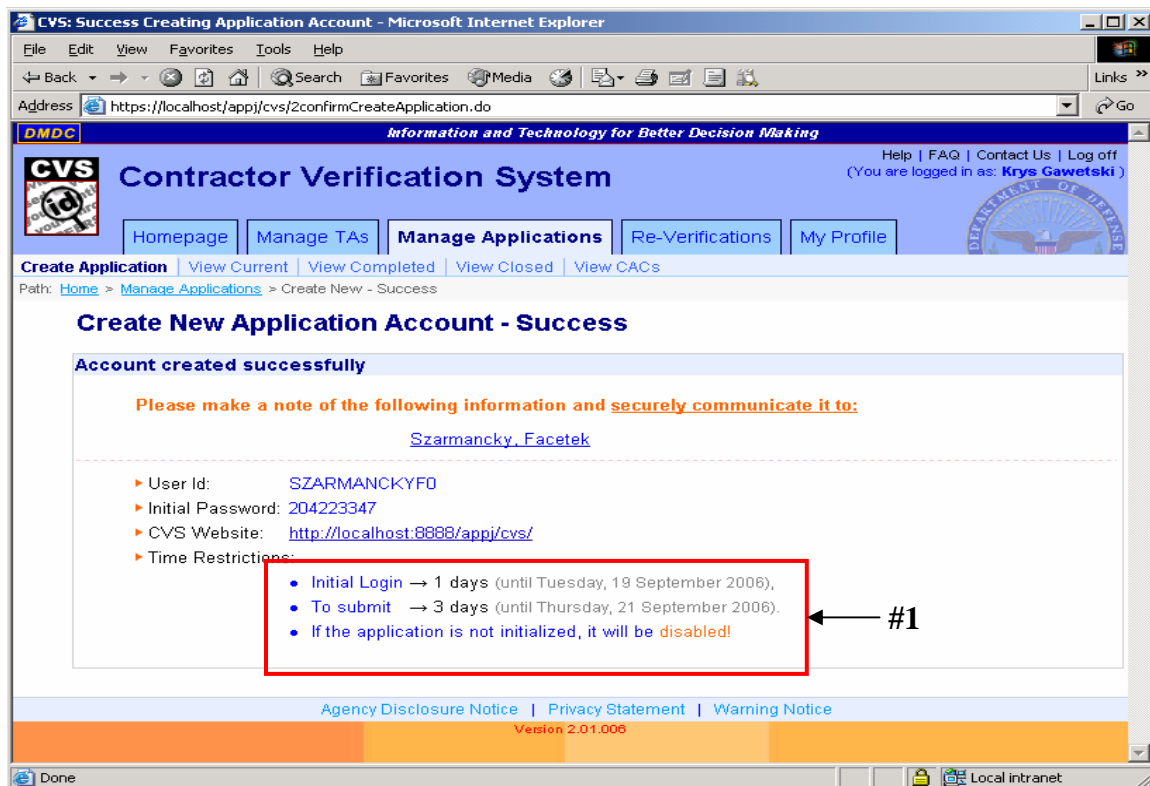
Figure 16 - Create New Application Account Success

6) As Trusted Agent, you are responsible for distributing the contractor's user account information (User ID and temporary password) to him or her in a secure manner.

> **CVS does not automatically notify (i.e. send an email to) a contractor when his/her account is first created. The TRUSTED AGENT is responsible for distributing the CVS WEB-SITE URL and the ACCOUNT INFORMATION using a separate and secure means.**

8.3   Managing Applications

1) To view current applications, view completed applications, view closed applications, and view CACs issued, click the "Manage Applications" link from the top row navigation. From the Manage Applications page, you may also access the screen for creating applications.

8.3.1   Viewing Current Applications

1) The View Current page supports the viewing of applications; the changing all current applications including those in progress, submitted, and returned; the disabling of application accounts; and the resetting of contractor passwords.
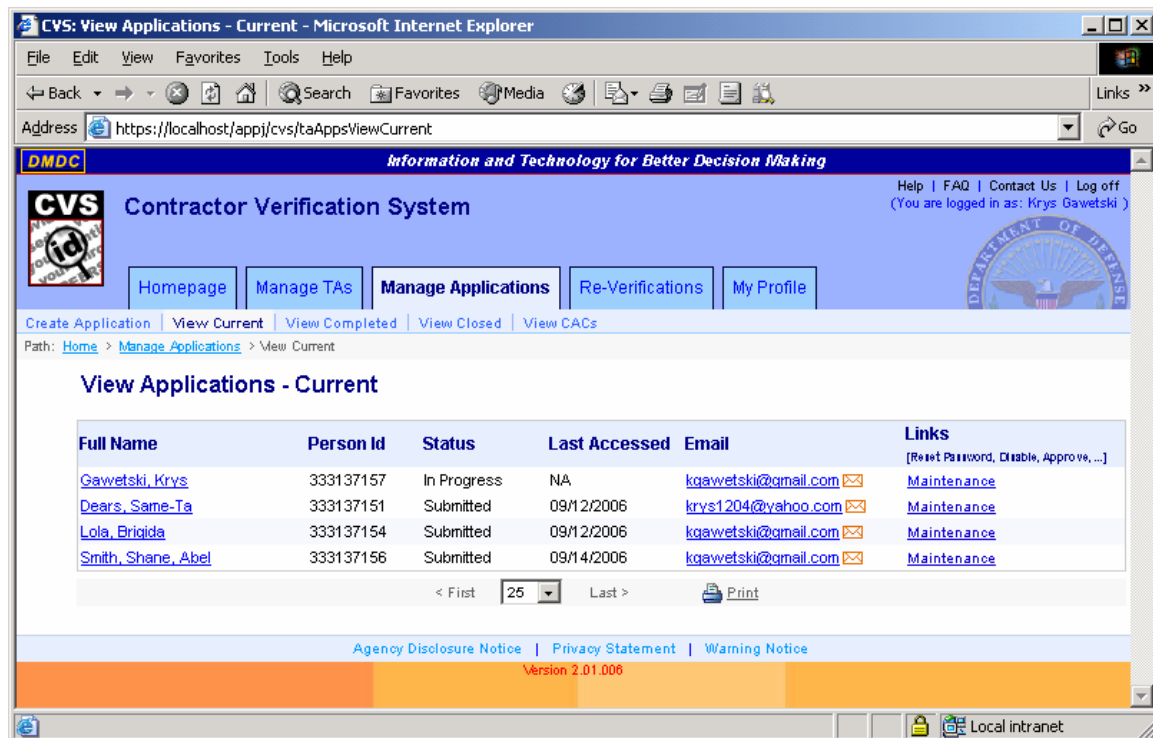
Figure 17 - View Applications – Current

2) Click the "View Current" button from the second row navigation.

3) To view a contractor's application only, click on the name in the Full Name column. To change an application, click the "Maintenance" link in the Links column.

4) When the contractor name is clicked, the "View Application" page will load in a new window (see Figures 18 and 19). From this page, you may only view the application and view the applicant's DEERS record, if it is available.[3] Changes to the application may only be made by selecting the "Maintenance" link in the Links column from the "View Applications – Current".

---

[3] DEERS contains records for contractors once their application is approved. New applicants, who have never received a CAC or been through the application process will not appear in the DEERS database until their application is approved.
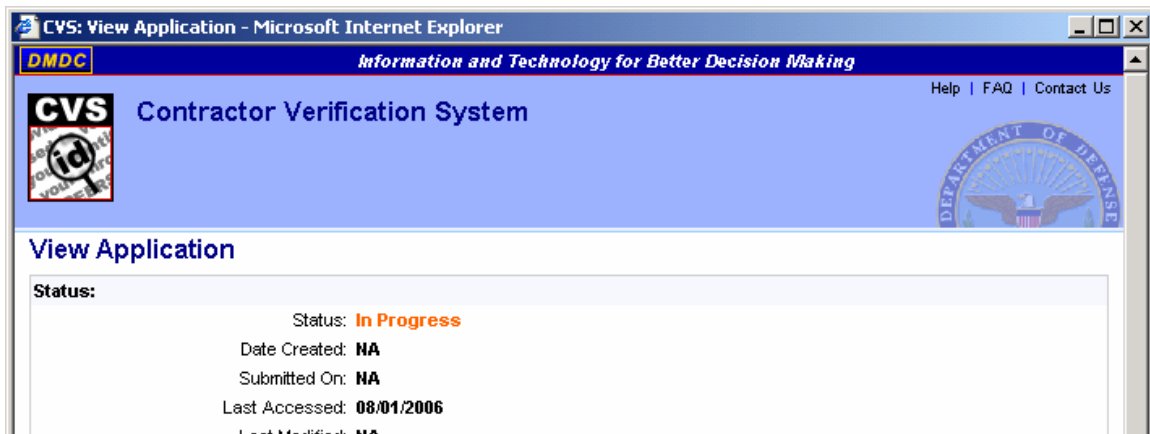
Figure 18 - View Application – upper section
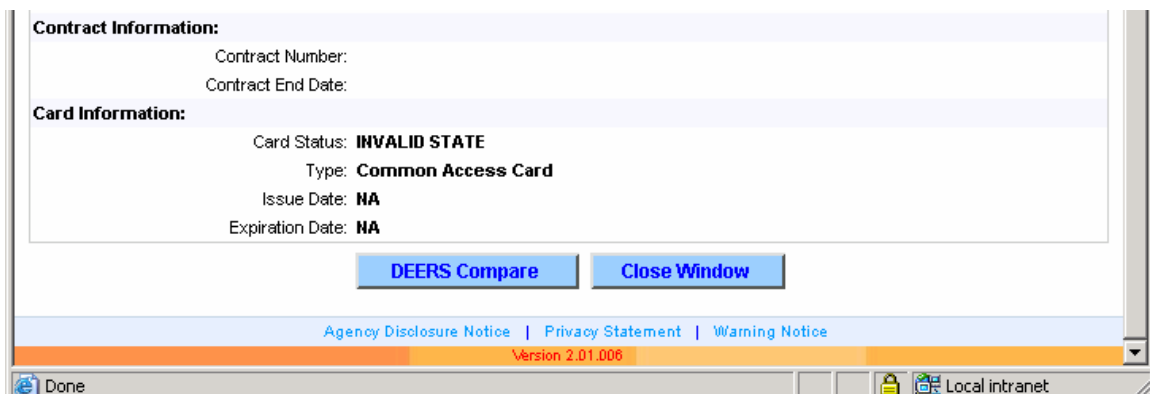
Figure 19 - View Application - lower section

5) When the "Maintenance" link is clicked, the "Application View/Maintenance" page will load in the main window. Depending on the status of the application, you may approve, reject, or return the application, disable the application account, or reset the contractor password from the "Application View/Maintenance" page. (Buttons at the bottom of the page, refer to actions that may performed to an application. The buttons: Approve, Reject and Return, Disable, and Reset Password are viewable depending on the status of the account. See Figure 20: "Button viewability based on status" and Figure 21.)

		In Progress	Approved	Submitted	Disabled	Returned	Rejected
Status of the Application							
Buttons/Actions	Disable	Yes	Yes[4]	Yes	No	Yes	No
	Approve	No	No	Yes	No	No	No
	Return	No	No	Yes	No	No	No
	Reject	No	No	Yes	No	No	No
	Reset Password	No	No	No	No	Yes	No

Figure 20 - Button viewability based on status
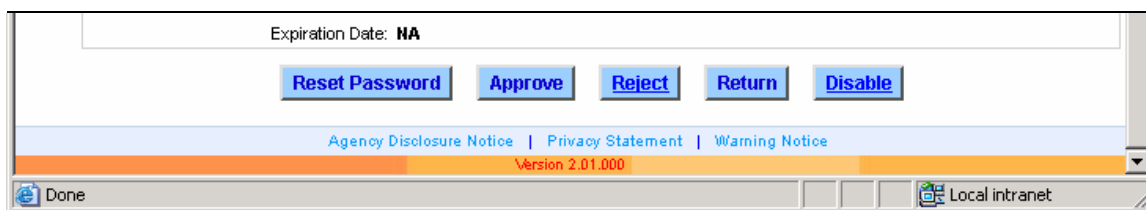
Figure 21 - Application View/Maintenance - lower half

6) When the "Approve" button is clicked, CVS will load the "Confirm Application Approval – CAC Exists" page (see Figure 22). From the page, you may approve a new CAC or retain an existing CAC if the previous card expired less than 90 days before.

---

[4] [1] TA should request assistance from CVS helpdesk for this option because this condition will lead to the termination of the personnel entry in DEERS associated with this application and the revocation of the certificates assigned to the CAC should there be a current CAC assigned.

Figure 22 - Confirm Application Approval

7) If you select either the "Reject" or "Return" button, CVS will load either the "Reject Application" or "Return Application" page respectively. Choose a reason from the available list of reasons on the page. Add any additional comments that you may deem necessary. When you are finished, click the "Reject Application" button. Click "Reset" to reset the form fields on the page. (See Figure 23.)
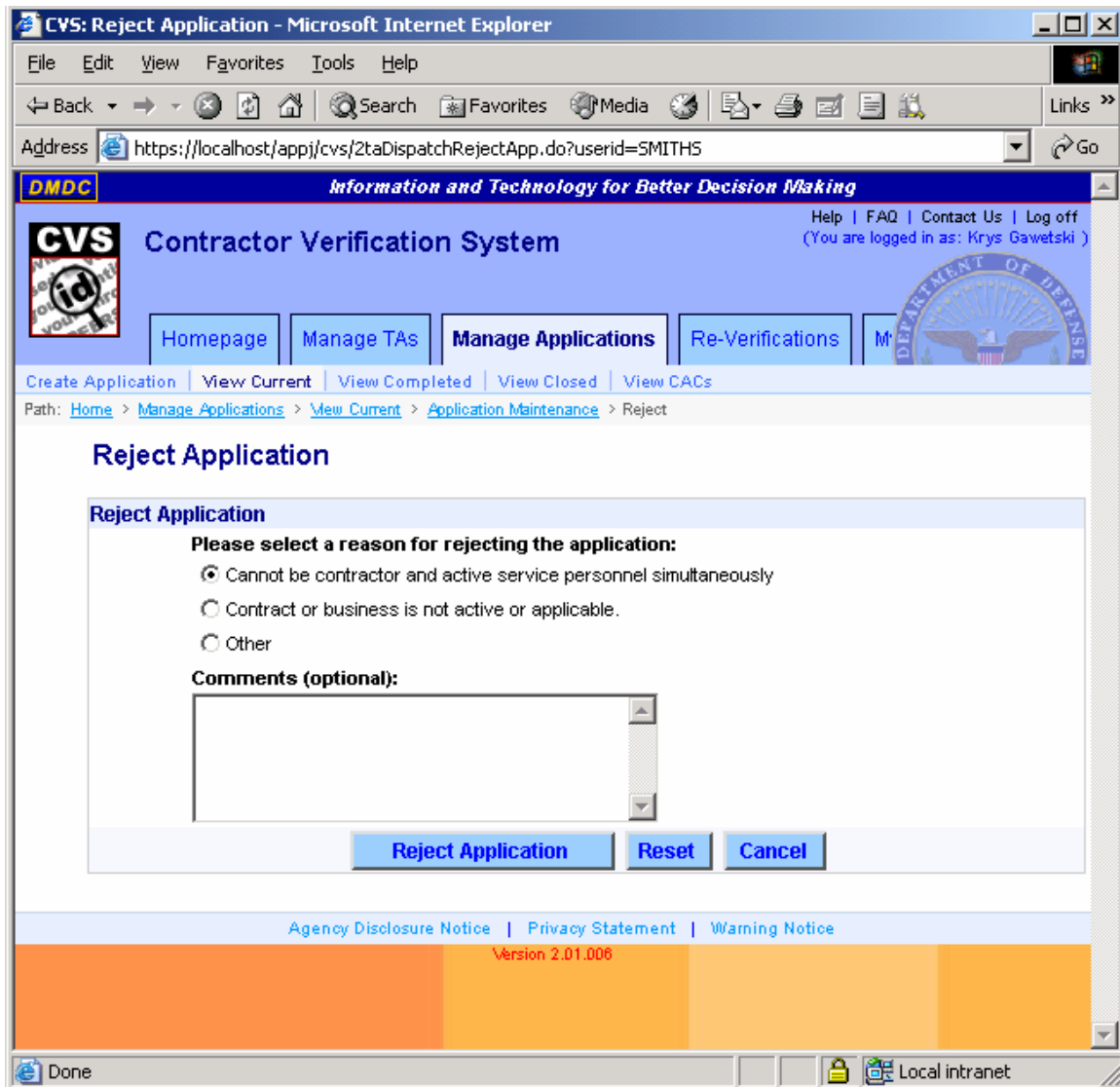
Figure 23 - Reject Application page

7) If you select the "Disable" button, the CVS will generate a pop-up window (see Figure 24) which asks you whether you would like to disable the application account.
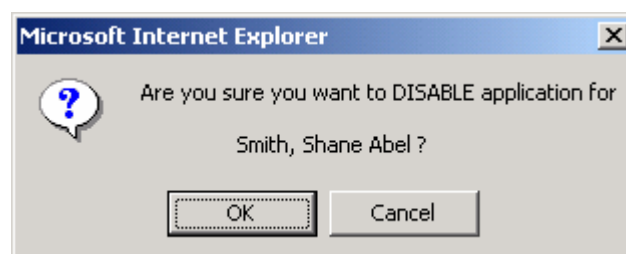
Figure 24 - Disable application window

8) When the "DEERS Compare" is clicked from the "View Application" page, the page will load with the applicant's information as it appears in the DEERS database. The page

will indicate if there was no information found in the DEERS database for the applicant (see Figure 25).

Figure 25 - DEERS Compare

8.3.2   Viewing Completed Applications

1) The "View Completed" page provides a link to contractor information concerning
applications which have *already* either been rejected or approved. To view these
applications, click the button labeled "View Completed" from the second row navigation.
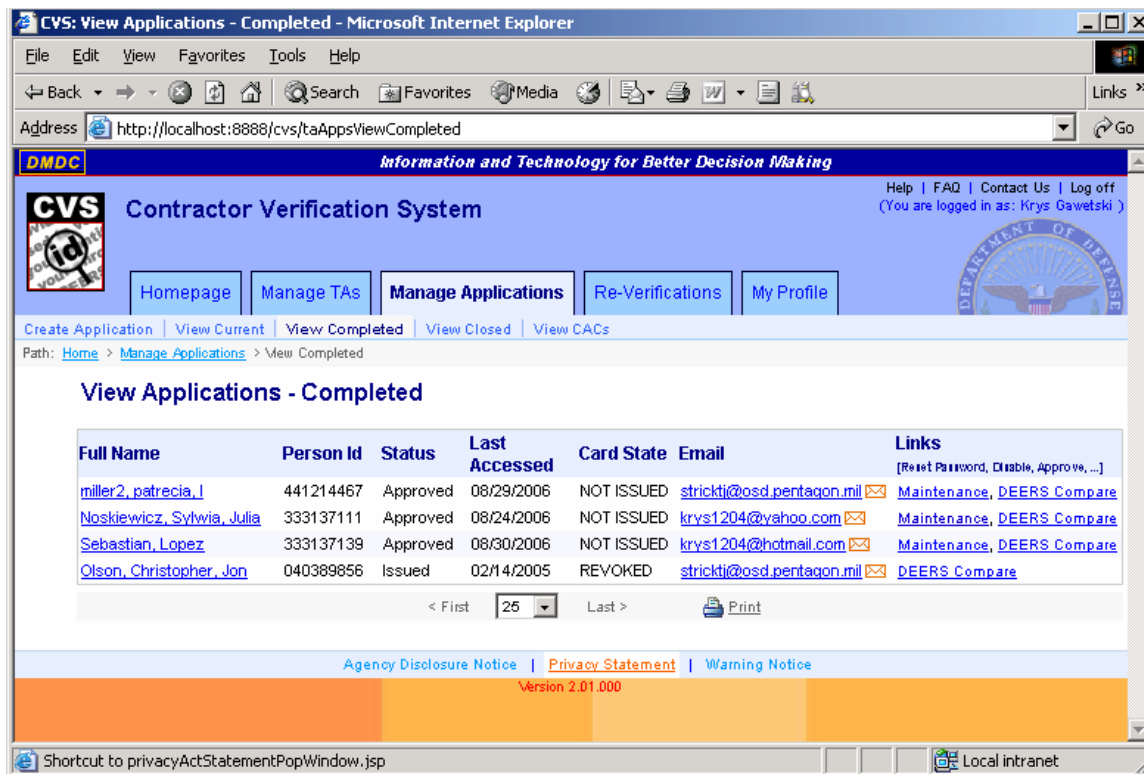
Figure 26 - View Applications – Completed

2) From the view applications completed screen, you may view the application details by
selecting a name from the Full Name column. You may make changes to the status of the
application by clicking "Maintenance" under the Links column. To compare the
contractor's application submittals with their DEERS record, click the link labeled
"DEERS Compare" in the Links column.

3) When the contractor name is clicked, the "View Application" page will load in a new
window (see Figures 18 and 19). From this page, you may only view the application and
view the applicant's DEERS record, if it is available.[5]

4) When the "Maintenance" link is clicked, the "Application View/Maintenance" page
will load in the main window. The page provides means to approve, reject, or return the
application, disable the contractor's account, or reset the contractor's password

---

[5] DEERS contains records for contractors once their application is approved. New
applicants, who have never received a CAC or been through the application process, will
not appear in the DEERS database.

depending on the status of the application. See Section 8.3.5 for more information on changing the status of an application.

8.3.3 Viewing Closed Applications

1) To view information for closed applications, click the second row navigation link labeled "View Closed".

Figure 27 - View Applications - Closed

2) From the "View Applications – Closed" page, you may view the application details, email applicants, and compare application data with data in the DEERS database. To view an applicant's application click the name in the Full Name column. To compare

application data with data from DEERS click the "DEERS Compare" link in the Links column.

8.3.4   Viewing Approved Applications

1) To view information for approved applications for which a CAC has been issued, click the link labeled "View CACs" from the second row navigation.
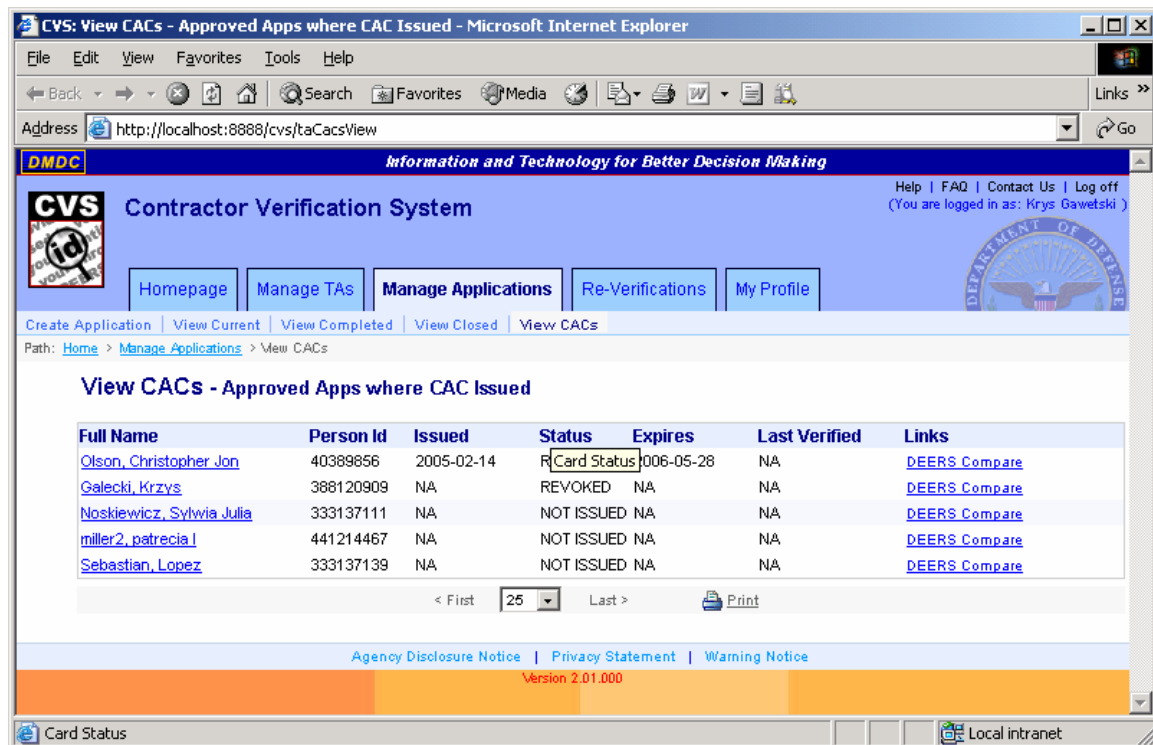
Figure 28 - View CACs

2) Click on the name in the Full Name column to access the approved application or the "DEERS Compare" link to compare the application data against data in the DEERS database as seen in Figure 25.

8.4   Resetting a Contractor Password

1) To reset contractor passwords, click one of the following links: "View Current", "View Completed", "View Closed", or "View CAC". When the page loads, click on the name in the Full Name column. The "View Application" page will load in a new window. Click on "Reset Password" at the bottom of the page (see Figure 29).

Figure 29 – View Application page - lower half

2) When the "Reset Password for Applicant" page loads, select the "Reset Password" button, taking care to acknowledge the name of the applicant displayed above (see Figure 30).
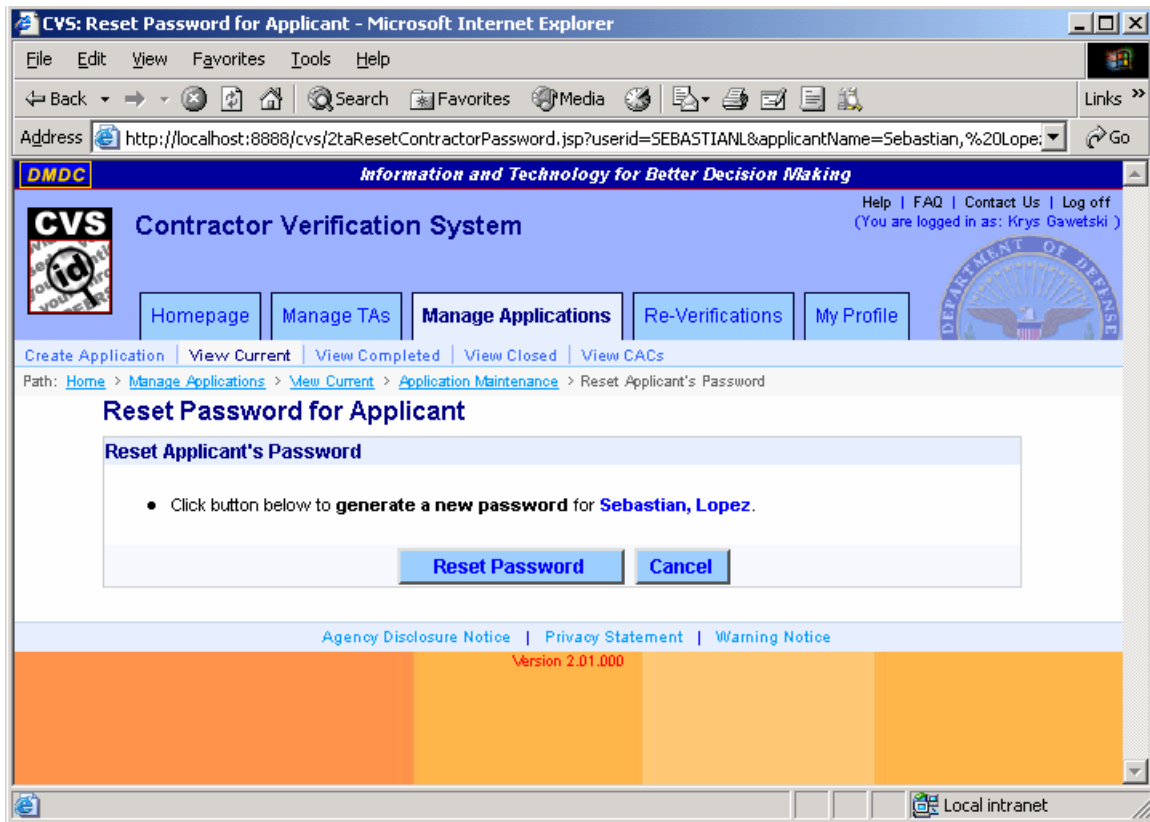
Figure 30 - Reset Password for Applicant page

5) When the password has been changed successfully, a confirmation page will appear with the new password. Distribute the new password to the contractor in a secure manner.
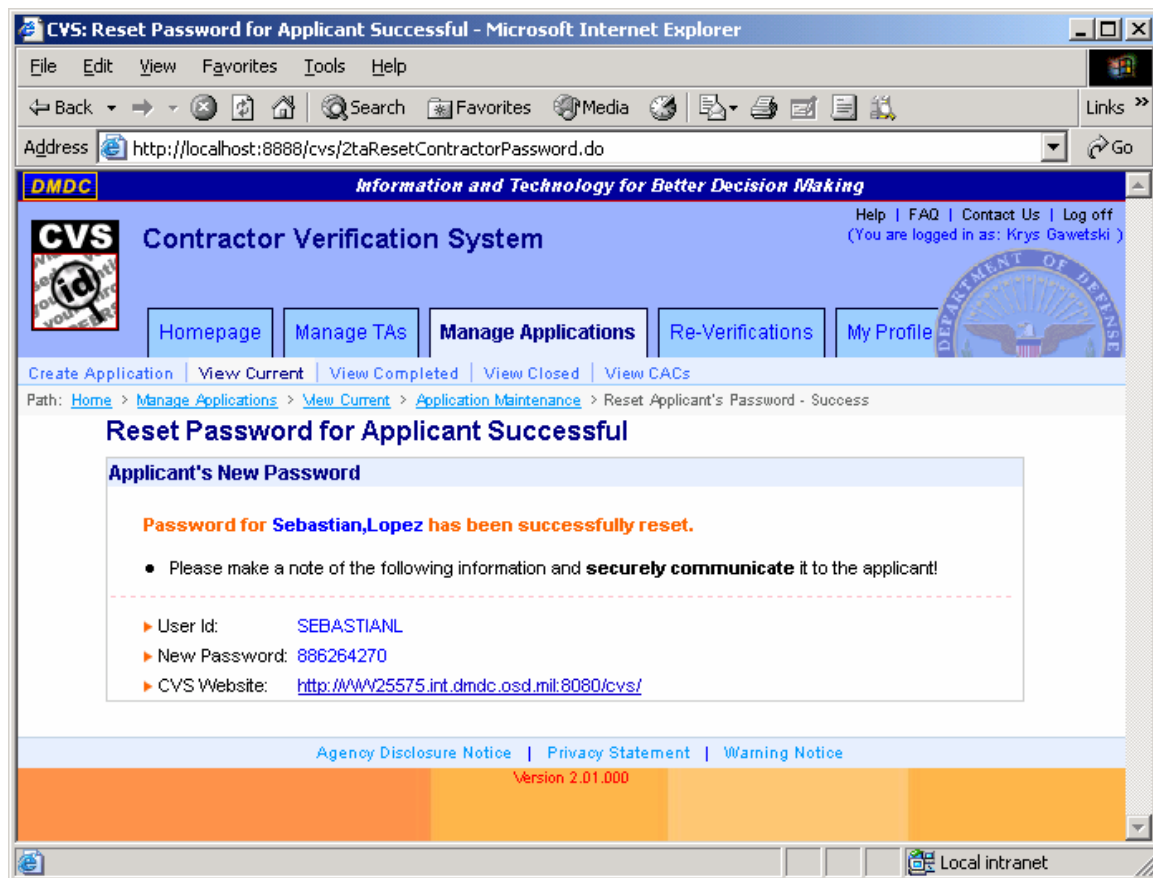
Figure 31 - Successful Reset of Applicant Password

8.5   Viewing Reverification Notices, Reverification, and Revoking CACs

1) Contractor privileges to use the CAC must be reverified every 180 days. The CVS will begin sending notice to reverify a contractor 30 days before the due date. You may also revoke CACs that have been issued to contractors who you sponsor using the "Reverification Notices" page.

2) To view contractor applications that require reverification, click the "Reverification Notices" from the navigation.

3) When the "Reverification Notices" button has been selected, the "TA Notices" page will appear displaying:

- Deadline by which time the reverification is to be performed
- Full name (Last, First name) of the Contractor
- Contractor person ID
- Date CAC was issued

- Date the contractor's CAC expires
- Contractor's CAC status
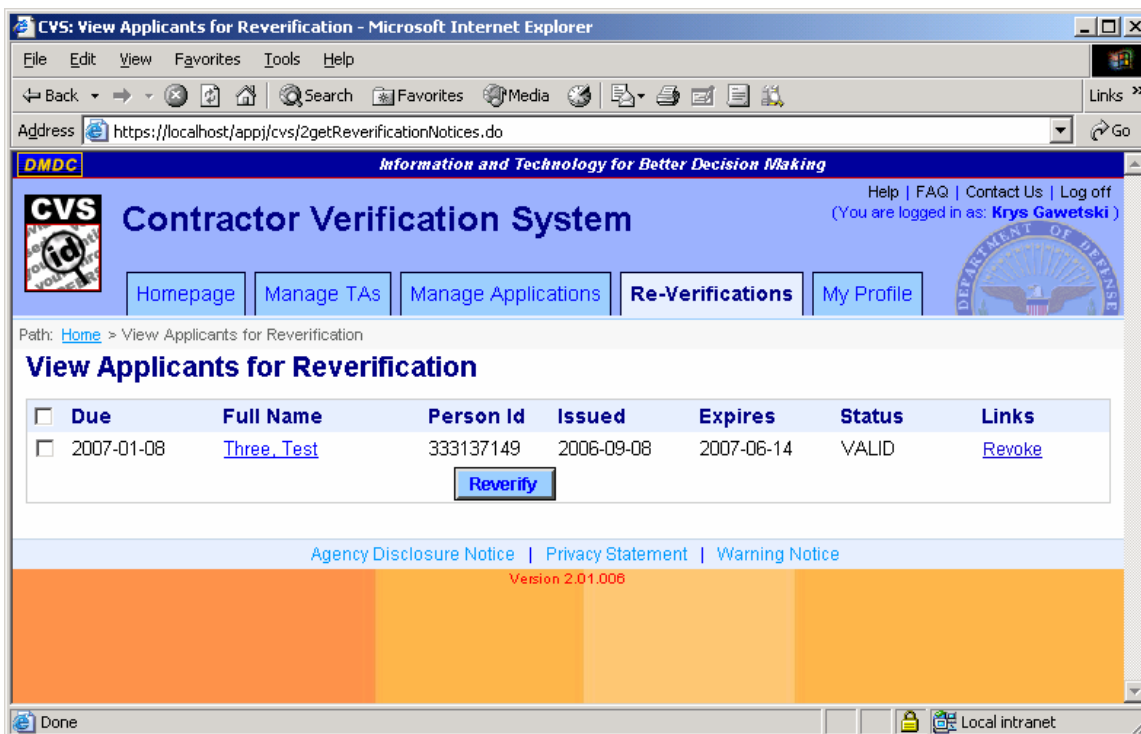
Figure 32 - View Applicants for Reverification

4) To reverify a contractor's authorization to hold a CAC, click on the "Reverify" button.

5) To revoke a contractor's CAC, click on the "Revoke" link in the Links column. When the link is clicked, a pop-up window (see Figure 33) will appear which asks whether or not you would like to revoke the contractor's CAC. When you make your selection, the system will load the "Revoke CAC" page which will report on the status of the request. (See Figure 34.)
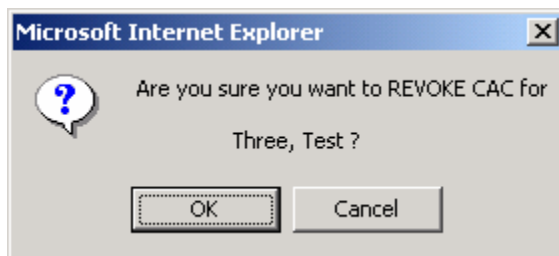
Figure 33 - Confirm Revoke Request
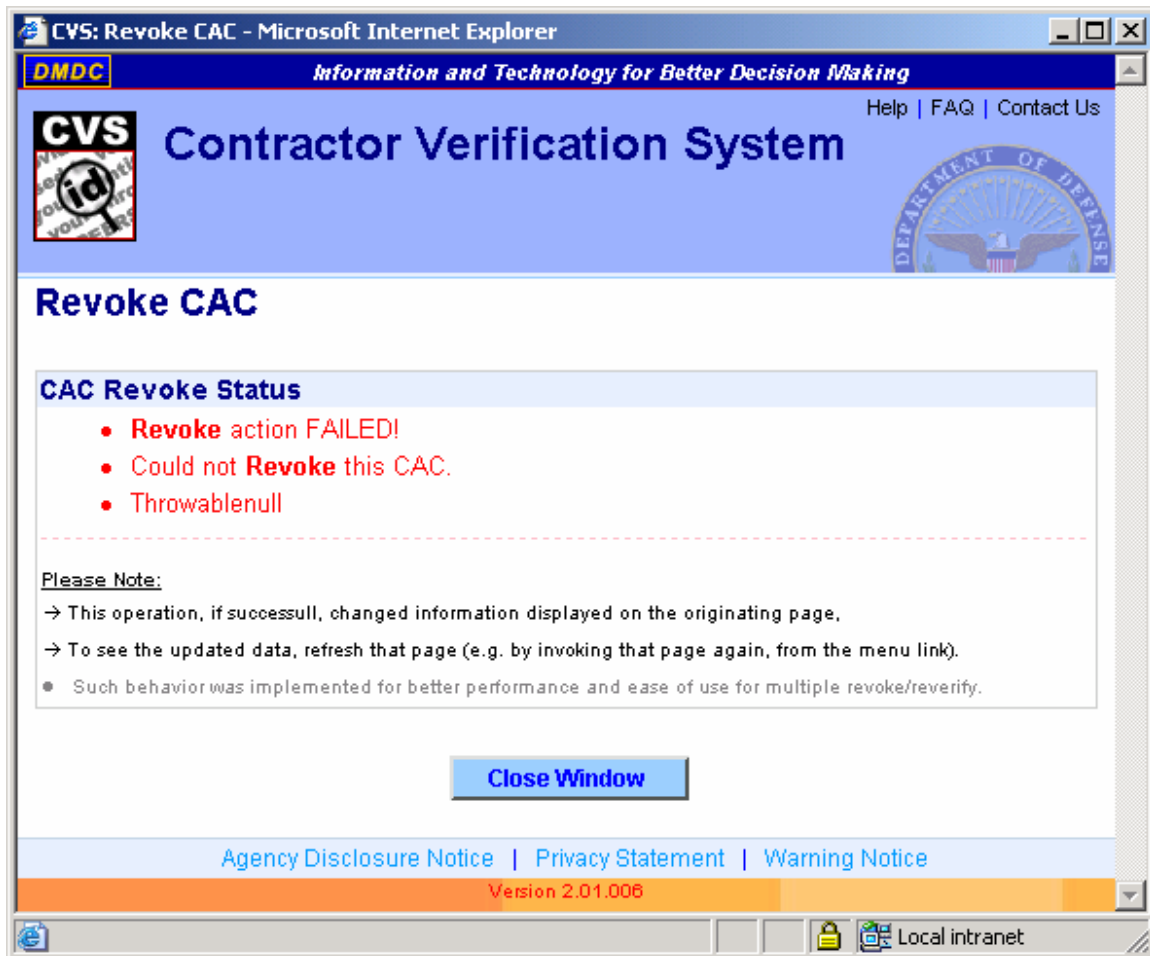
Figure 34 - Revoke CAC page

8.6 Updating Your TA Profile

1) To update your account information, select the "My Profile" button from the top row navigation. The "TA Edit Profile" page will load which allows you to make changes to your contact information and password (see Figure 35). Click the +/- toggle button to alternately hide or display the contact or password information.

Figure 35 - TA Edit Profile

2) To change contact information, enter and confirm preferred new e-mail address and/or your first, middle and last name. Click the "Save" button to submit changes. To change your street address, click the link:

https://www.dmdc.osd.mil/address/index.jsp.

The link will open the Address Update homepage. To access Address Update site location, you will need to provide CAC, registered user information, or personal information as designated by the site.

3) To change your password, enter your old password and your preferred new password in the space provided. Re-enter your new password to confirm your selection. Be sure to follow the established password format: 8 characters in length, 1 character upper case, 1 character lower case, at least one special character, no repeating character repeating more than twice, not matching any of the previous 5 passwords. When finished, click on the "Change Password" button.

4) When the password has been successfully changed, a screen confirming the successful change will appear.

9   Contractor User Guide

9.1   Contractor Log in

1) To log into the CVS site, you will need to enter the user ID and password provided by your TA. The TA will also provide information regarding the number of days remaining to log in and to fill out and submit the application.

2) You will see the "Privacy Act" page when user ID and password are entered correctly. Select "I Agree" to proceed. Click "I Do Not Agree" if you do not wish to proceed.

3) At first successful log in, you will be directed to the "Change Password First Time" page, where you will be directed to change your password (see Figure 36).

Figure 36 - Contractor Change Password

4) Enter the old password (provided by the TA) and a preferred new password, taking care to follow the established password format: 6-8 characters, mixed-case, 1 number, and 1 special character. Re-enter the new password to verify your choice. (A contractor may request a password change from a TA at any time.) When finished, click the "Change Password" button. **You will be redirected to this page until you change your password.** If your account has been suspended, you will receive notification of the fact on the log in page.

5) When the new password is received, the "Applicant Homepage" loads.
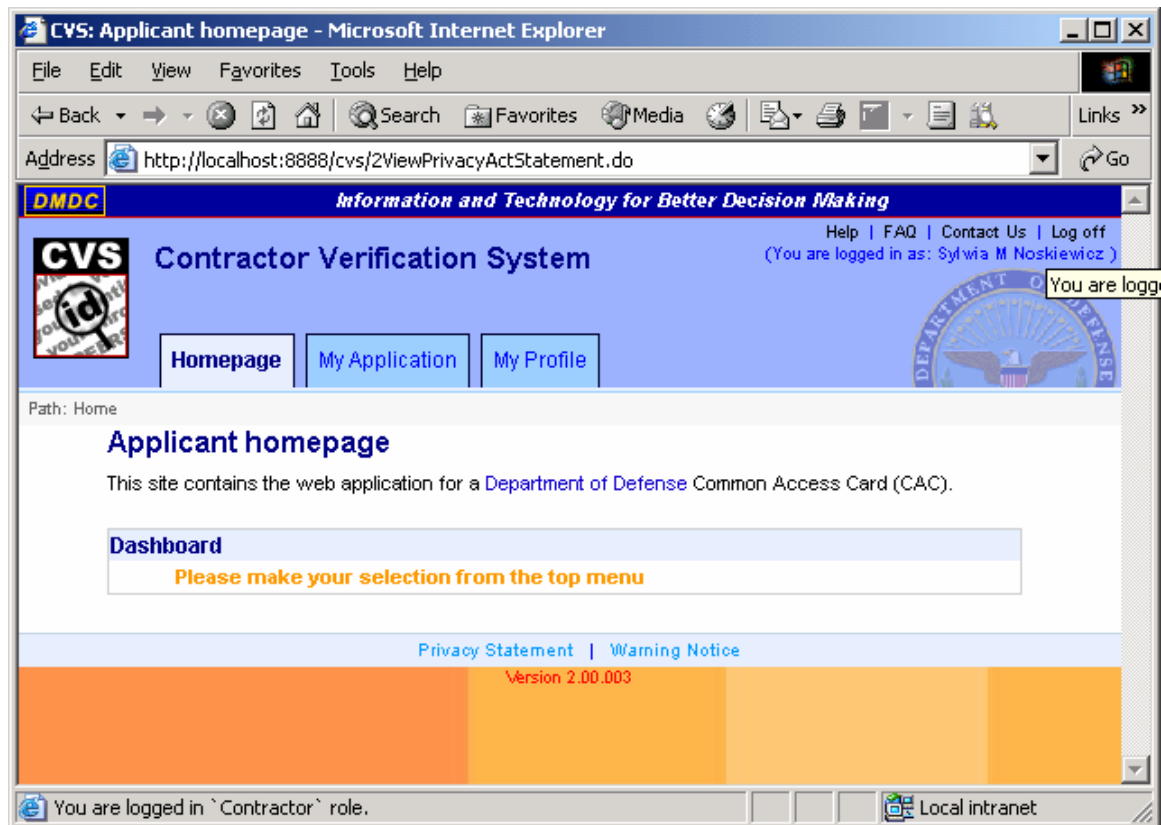
Figure 37 - Applicant home page

9.2   Starting and Saving an Application

1) From the top row navigation, select the "My Application" link.
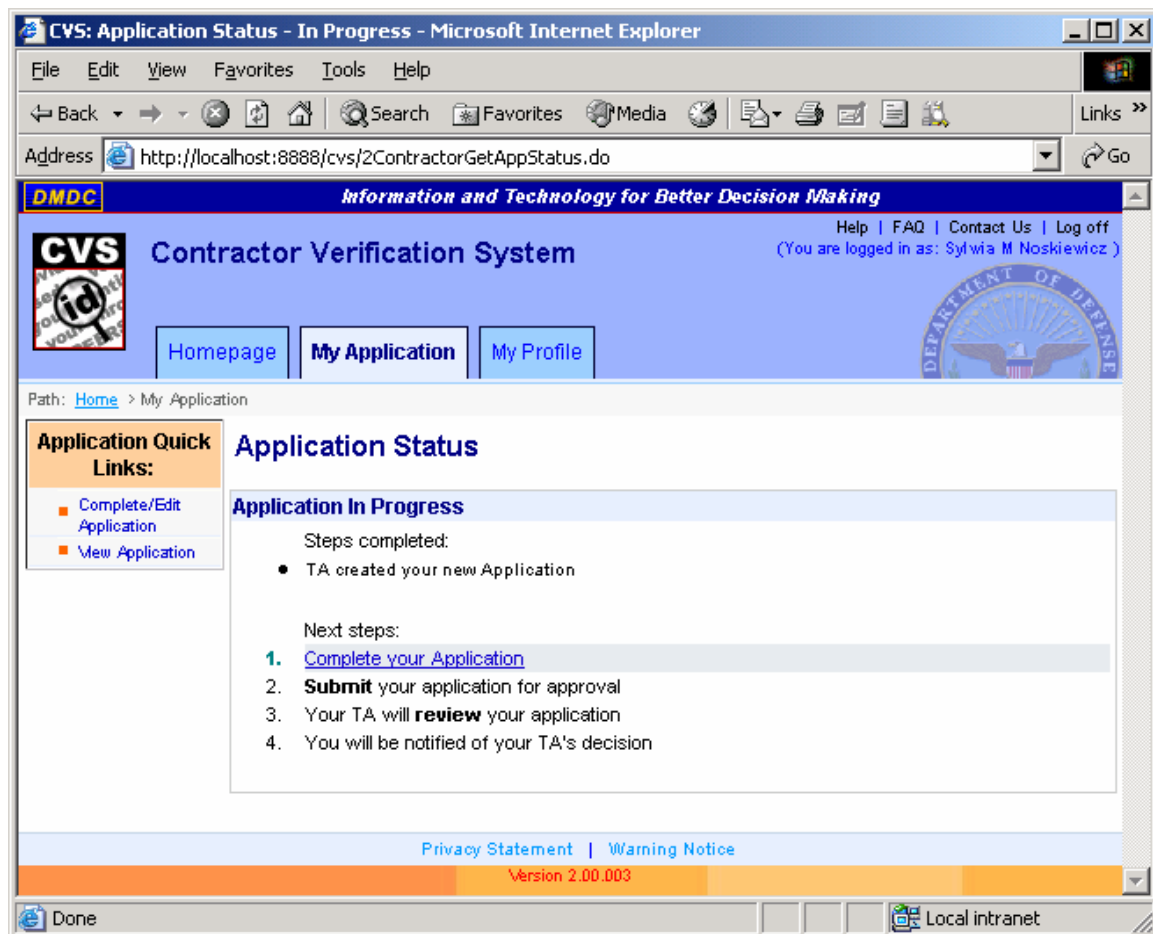
Figure 38 - Application Status page

2) A screen will appear indicating the status of the application, steps completed, and next steps to take toward completion of the application. To start an application, click the "Complete your Application" link as indicated in Figure 38.

3) When the "Complete/Edit Application" page appears, supply the appropriate information. When you complete the application, click the "Submit for Approval" (see Figure 40) button at the bottom of the form to submit to your TA. If you have not completed the application and want to save the entries that you have made, click the "Save without Submitting" button at the bottom of the page. The system will return a "Application Saved" page to confirm that the save request is successful (see Figure 41). See "Edit a Saved Application" (Section 9.3) to complete the application at a later time. To cancel an application, click "Cancel".

Figure 39 - Complete/Edit Application - upper half

Figure 40 - Complete/edit Application - lower half

4) CVS checks the form for missing or incorrect information when the application is submitted. If the CVS detects errors in the completion of the form, it will generate an error page that prompts you to make the necessary corrections to complete the application for submittal. The system will generate error pages until the information requested is entered correctly. The error page may be saved, submitted, or cancelled by using the buttons located at the bottom of the page (see Figure #31).

AN APPLICATION WILL NOT BE SENT TO THE TRUSTED AGENT FOR REVIEW UNTIL THE SUBMIT BUTTON HAS BEEN CLICKED.

A CONTRACTOR HAS 7 DAYS FROM WHEN THE TA CREATED AND SUBMITTED THE APPLICATION TO LOG IN AND CHANGE THE PASSWORD OR CVS WILL DISABLE THE CONTRACTOR ACCOUNT. AFTER THE INITIAL LOGIN THE CONTRACTOR HAS UP TO 30 DAYS, INCLUDING THE 7 DAY LOG IN TIMEFRAME, TO FILL OUT AND SUBMIT AN APPLICATION, AFTER WHICH CVS WILL AUTOMATICALLY DISABLE THE APPLICATION AND REQUIRE THE TRUSTED AGENT TO CREATE A NEW CONTRACTOR ACCOUNT TO BEGIN THE APPLICATION ANEW.
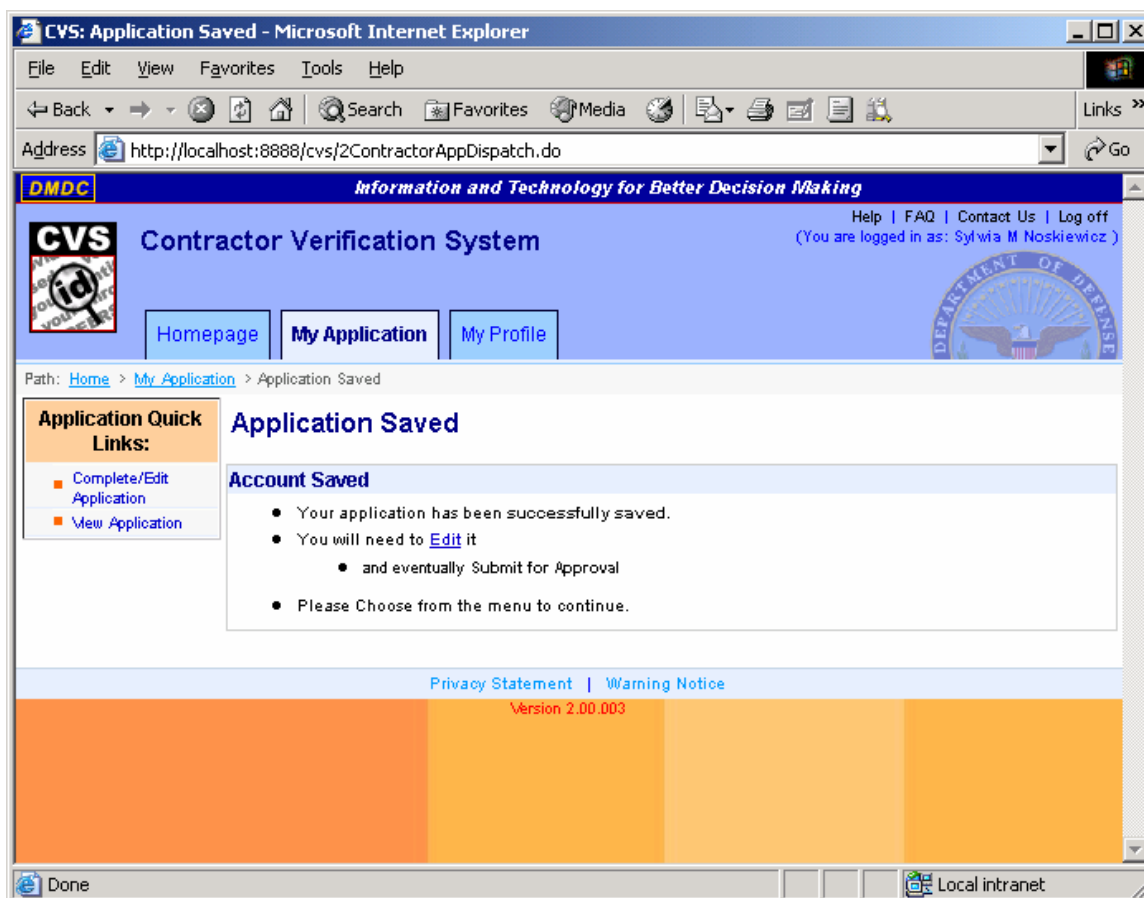
Figure 41 - Application Saved

5) When all required information has been entered and submitted, an **"**Application Confirm" page will appear. Review the page and select "Confirm" if the information is correct or "Cancel" to return to the application to make any necessary changes.

6) When the "Confirm" button is clicked, a page is generated that reports on the success of the confirmation. Once you confirm the application, you will no longer be able to access your application. The system automatically notifies the TA via e-mail that your application is ready for review.

9.3 Editing a Saved Application

1) To resume completion of a saved application, select "Edit Saved Application" link as it appears on the "Application Status" page (see Figure 38).

2) When the "Edit Saved Application" button is selected, the "Saved Application" page will appear. Complete the form as indicated. Click "Submit" when complete. The system will return the form if it is not completed as required. Complete the form, taking note of corrections to be made. To re-save a partially completed application, click "Save without Submitting" at the bottom and return to Step 1 of this section.

3) If the application is saved rather than submitted, a page will confirm that the application has been saved successfully.

4) If the application is submitted and CVS detects missing or incorrect information, the system generates an error page. The system will generate error pages until the information requested has been entered. The error page may be saved, submitted, or cancelled at any time during the correction process using the buttons located at the bottom of the page.

5) When all required information has been entered and submitted, a page is generated that confirms that the application has been submitted successfully. Once the application has been successfully submitted, you will not be able to edit the application unless the Trusted Agent returns the application to you for correction. For editing a returned application, see Section 9.4. The browser application must be closed to complete all transactions and to protect data integrity. The system automatically notifies the TA via e-mail that an application has been submitted and is ready for review.

9.4 Editing a Returned Application

1) If the reviewing TA returns the application, a notice that the application has been returned will appear when you select the "My Application" page from the top row navigation.
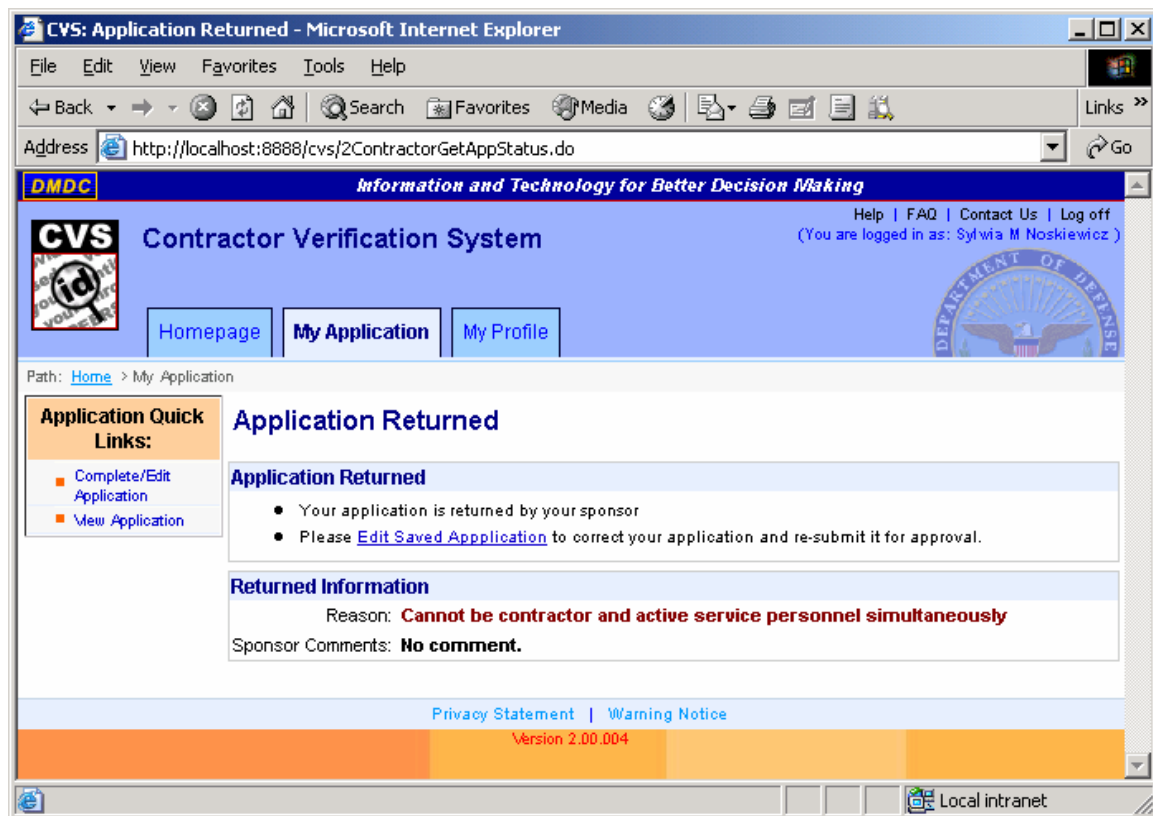
Figure 42 - Application Returned

2) Read the information regarding the reason for the returned application. If the reason for the return indicates specific steps to be taken to complete the application, click "Edit Saved Application" and proceed accordingly.

9.5   Rejected Application

1) If the application is rejected, a notice of rejection will appear when you select the "My Application" page from the top row navigation bar. Please read the rejection information provided. Contact your TA for further information. You may view the application; however, no updates may be made.
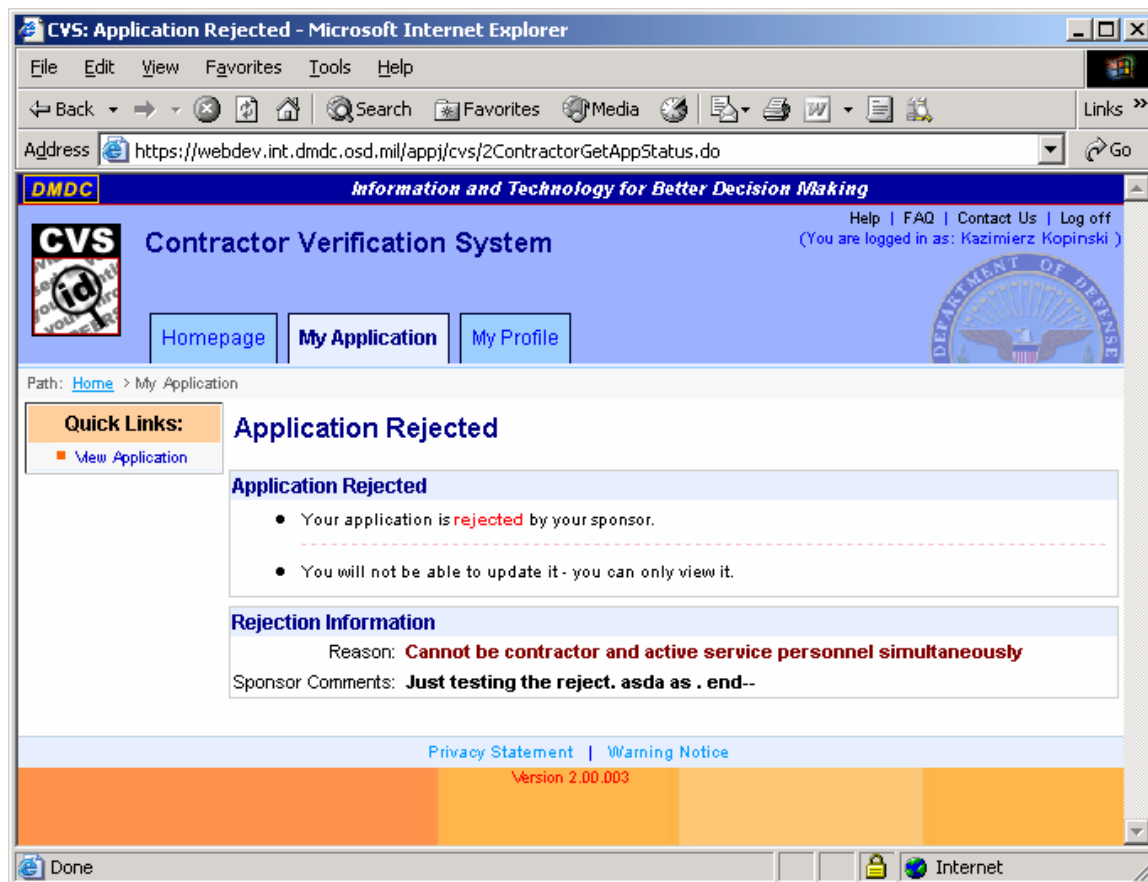
Figure 43 - Application Rejected

9.6 Post-application/Account auto-disabled

1) When the application process has been completed, the contractor's CVS account is automatically disabled and the application is no longer accessible. After the account is disabled, the Contractor Account Disabled page will appear every time a log in is attempted.
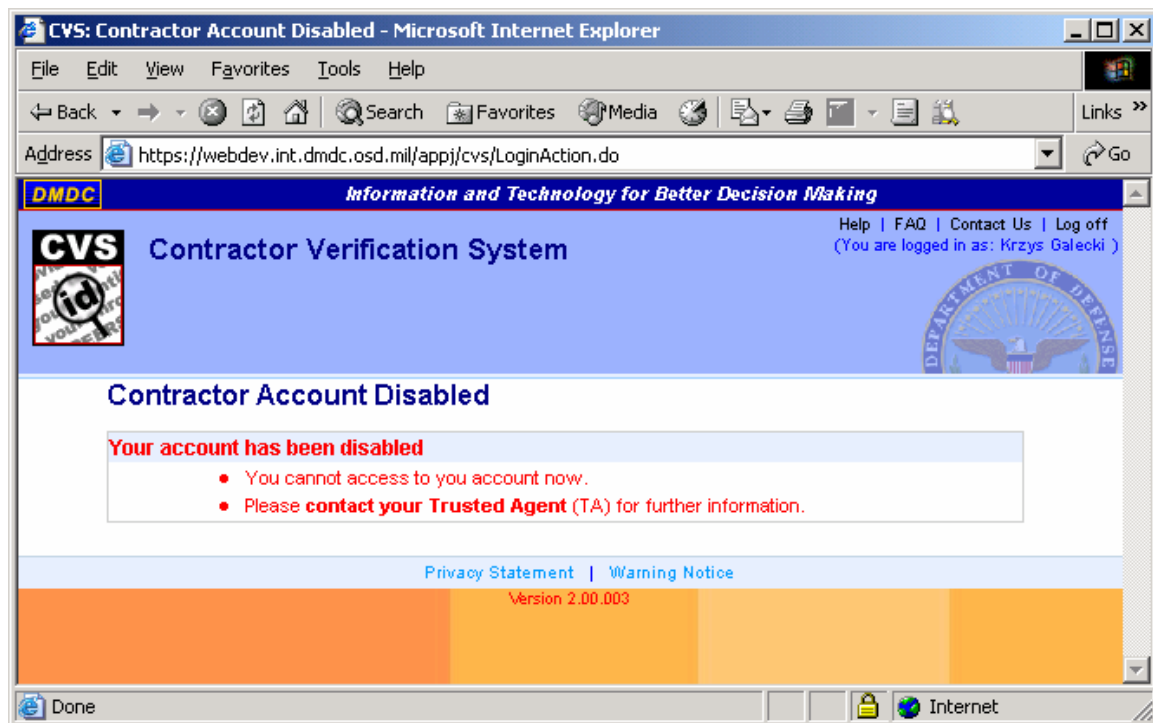
Figure 44 - Contractor Account Disabled

9.7 Editing Your Profile (Change Password or Contact E-mail)

1) To edit your profile, select "**My Profile"** from the top row navigation,.

2) When the "My Profile" button is clicked, a page will appear providing fields to update current contact information and password. Click the toggle button as indicated in Figure 45 to alternately hide or show either the contact or the password information and update form.
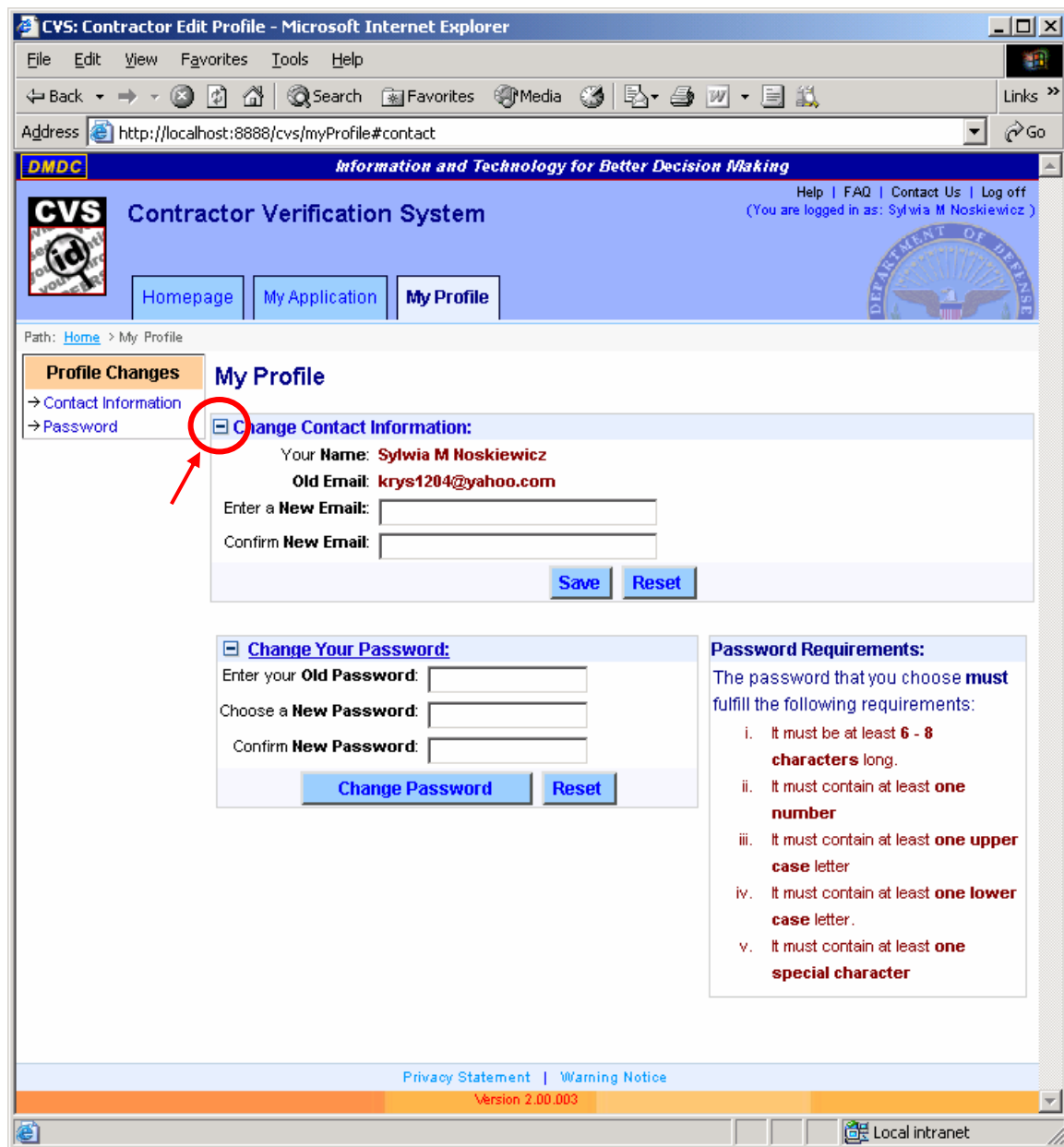
Figure 45 - My Profile page

3) To change the contact e-mail, enter your preferred new e-mail address in the space provided. Re-enter your new e-mail address to confirm your entry. Click the "Save" button to request the change.

4) When the e-mail address has been successfully changed, a screen confirming the successful change will appear. Select an option and continue using the CVS site or log off by closing the browser application.

5) To change your password, enter your old password and your preferred new password in the space provided. Re-enter your new password to confirm your selection. Take care

to follow the established password format: 6-8 characters, mixed case, one number, and one special character. Click the **"**Change Password**"** button to request the change.

6) When the password has been successfully changed, a screen confirming the successful change will appear.

10 Personnel Controls

10.1 Background, Qualifications, Experience, and Clearance Requirements

CVS managers and users must meet the requirements listed in sections 5.2 through 5.4.

10.1.1 SPOC

The CVS SPOC must:

- Be a U.S. Citizen

- Be a DoD uniformed service member, DoD civilian, or contractor working for the Service/agency

- Be capable of sending and receiving digitally signed and encrypted email. Be a CAC holder.

- Be a CAC holder

- Have a working knowledge of Service/agency structure, including populations and missions of Service/agency posts and sites

- Be familiar with Public Key Infrastructure (PKI), the CAC issuance process, and the Service/agency's CVS process policy

- Have not been convicted of a felony offense

- Have had a National Agency Check (NAC) background investigation performed

- Have not knowingly been denied a security clearance or had a security clearance revoked

- Be trustworthy

- Be retainable for a minimum of 12 months.

10.1.2 TASM

A Trusted Agent Security Manager must:

- Be a U.S. Citizen

- Be a DoD uniformed service member or DoD civilian working for the Service/agency

- Be capable of sending and receiving digitally signed and encrypted email

- Be a CAC holder

- Have a working knowledge of the structure of the site under their control, including unit populations and missions

- Have had a National Agency Check (NAC) background investigation performed

- Have completed CVS TASM training

- Have not been convicted of a felony offense

- Have not knowingly been denied a security clearance or had a security clearance revoked

- Be trustworthy

- Be retainable for a minimum of 12 months.

10.1.3 TA

- A CVS Trusted Agent must:

- Be a U.S. Citizen

- Be a DoD uniformed service member or DoD civilian working for the Service/agency

- Be a CAC holder

- Have completed hands-on CVS training (administered by the site TASM) or another TA

- Have not been convicted of a felony offense

- Have not knowingly been denied a security clearance or had a security clearance revoked

- Be trustworthy.

11 Appendix A: Form 1172-2

Please read Agency Disclosure Notice, Privacy Act Statement, and Instructions prior to completing this form.

DD FORM 1172-2, OCT 2002   Reset

This form valid for issue of Common Access Card for 90 days from date of verification.
REPLACES DD FORM 1172-2 TEST, WHICH IS OBSOLETE AS OF DECEMBER 1, 2002.

AGENCY DISCLOSURE NOTICE

The public reporting burden for this collection of information is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0415), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THIS ADDRESS.
RETURN COMPLETED FORM TO A REAL-TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM WORK STATION.

PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. Section 301; 10 U.S.C. Sections 1074(c)(1) and 1095(k)(2); 10 U.S.C. chapter 147; 50 U.S.C. chapter 23; E.O. 9397; E.O. 10450, as amended.

PRINCIPAL PURPOSE(S): To apply for the Common Access Card and/or DEERS Enrollment; control access to and movement in or on DoD installations, buildings, or facilities; regulate access to DoD computer systems and networks; and verify eligibility, if authorized, for DoD benefits or privileges. To authenticate the identity of the authorizing/ verifying official for security or auditing purposes.

ROUTINE USE(S): To Federal and State agencies and private entities, as necessary, on matters relating to utilization review, professional quality assurance, program integrity, civil and criminal litigation, and access to Federal government facilities, computer systems, networks, and controlled areas.

DISCLOSURE: Voluntary; however, failure to provide information may result in denial of a Common Access Card; non-enrollment in the Defense Enrollment Eligibility Reporting System (DEERS); refusal to grant access to DoD installations, buildings, facilities, computer systems and networks; and denial of DoD benefits and privileges if otherwise authorized.

[For contractor personnel who are not required to have a National Agency Check only: Failure to provide a social security number will not result in denial of the Card, enrollment in DEERS, access to facilities or networks, or if eligible for, receipt of DoD benefits and privileges (other than non-emergency health care services), provided alternative means of identification (original birth certificate, passport, etc.) are voluntarily furnished upon request. However, submission of alternative identification may cause substantial delays; and if not provided, may result in denial of the Card, non-enrollment, refusal of access, and denial of benefits and privileges.]

INSTRUCTIONS

Instructions for the DD Form 1172-2 can be found at:
http:www.dmdc.osd.mil/smartcard/docs/1172-2_Instructions.pdf

DD FORM 1172-2 (BACK), OCT 2002

12 Appendix B: Form 1172-2 Instructions

INSTRUCTIONS FOR COMPLETION OF DD FORM 1172-2, "APPLICATION FOR DEPARTMENT OF DEFENSE COMMON ACCESS CARD – DEERS ENROLLMENT", April 2001 Version

The DD Form 1172-2 shall be used to apply for issuance of United States Dodd/Uniformed Services Geneva Conventions Identification Card for Civilians Accompanying the Armed Forces, the United States DoD/Uniformed Services Identification and Privilege Card, the United States DoD/Uniformed Services Identification Card and for enrollment or update of eligible individuals into the DEERS data base. This form is to be used primarily for initial DEERS enrollment of new civilian employees prior to their enrollment in DEERS, for DEERS enrollment and verification of continued association with the Department of Defense for contractor employees, and for individuals eligible for a CAC who are not enrolled in DEERS. Retention and disposition of the DD Form 1172-2 shall be in accordance with the Uniformed Services' regulatory instructions.

Members of the Uniformed Services, their family members and Retirees of the Uniformed Services shall continue to use DD Form 1172.

Mark here for civilian or contractor pre-eligibility: Mark with X, if purpose of the form is for DEERS enrollment, not for immediate issuance of CAC.

SECTION I – EMPLOYEE INFORMATION
Block 1. Name. Enter the employee's LAST name first, enter the FIRST name, and then enter the MIDDLE INITIAL or the full MIDDLE NAME. (Use no more than 51 characters.)

> The name field can include a designation of JR, SR, ESQ, or the Roman numerals I through X. To include that designation, enter the appropriate data after the middle initial. The name cannot contain any special characters nor is any punctuation permitted.

Block 2. Sex. Enter the sex of the employee from the valid abbreviations listed in the left column, below: (Use one character.)

> M - Male
> F – Female

Block 3. Social Security Number (SSN). Enter the employee's SSN. In cases where the employee does not have an SSN, a number will be generated by the system. A Foreign Identification Number (FIN) (assigned as 900-00-0000F and up) will be assigned and

automatically generated for eligible foreign military, foreign nationals who do not have an SSN, and contractor employees who refuse to provide their SSN. (Use nine characters, 10 characters in the case of a FIN.)

> If the SSN is already registered on the DEERS database for another individual, STOP processing and verify the number. If verification confirms duplication of the SSN by the Social Security Administration, continue processing and the system shall automatically generate a duplicate control number for the additional employee.

Block 4. Status. Enter the correct abbreviation for the status of the employee from the valid abbreviations listed in the left column, below: (Use no more than six characters.)

> CIV   - Civilian employee
> CONTR - Contractor employee
> FN   - Foreign national personnel
> FP   - Foreign military personnel
> OTHER - Non DoD-eligible individuals

Block 5. Organization. Enter the correct organization with which the employee is affiliated from the valid abbreviations listed in the left column, below: (Use no more than five characters.)

> USA   - the U.S. Army
> USN   - the U.S. Navy
> USAF   - the U.S. Air Force
> USMC - the U.S. Marine Corps
> USCG - the U.S. Coast Guard
> USPHS - the U.S. Public Health Service
> NOAA - the National Oceanic and Atmospheric Administration
> DOD   - Department of Defense
> OTHER - used when the individual is not affiliated with one of the Components listed above

Block 6. Pay Grade. Enter the correct employee pay grade from the valid abbreviations listed in the left column, below. (Use no more than four characters.)

> GS01-GS15   Federal employees with General Schedule pay grades
> SES   Senior Executive Service Personnel
> EXEC   Executive Level Personnel
> NF1-NF6   Federal employees with Nonappropriated Fund pay grades
> GSE01-GSE15 General Schedule Equivalent to be assigned to contractor personnel
> OTHER   Other (non-Uniformed Service) pay grades not defined above
> N/A   Not applicable. Use this code with the Block 4 status codes

Block 7. GEN CAT (Geneva Convention Category). Enter the employee's appropriate Geneva Convention Category from the valid abbreviations listed in the left column, below. That block is automatically generated for online systems. (Use no more than three characters.)

I	Category I (GS-1 through GS-4, WG-1 through WG-8, WP-4 through WP-10, NF-1 and NF-2).
II	Category II (GS-5 and GS-6, WS-1 through WS-7, WL-1 through WL-5, WG-9 through WG-11, WP-11 through WP-16, and NF-3).
III	Category III (GS-7 through GS-11; WS-8 through WS-13, WL-6 through WL-14, WG-12 through WG-15, WP-17, 18, and Production Support Equivalents, NF-4).
IV	Category IV (GS-12 through GS-15, Ships Pilots, WS-14 through WS-19, WL-15, and Production Support Equivalents, NF-5). V Category V (SES and EXEC, NF-6).
N/A	Not applicable (nonprotected personnel)

Block 8. Citizenship. Enter the employee's appropriate country of citizenship.

Afghanistan AF	Albania AL
Algeria AG	America Samoa AQ
Andorra AN	Angola AO
Anguilla AV	Antarctica AY
Antigua and Barbuda AC	Argentina AR
Armenia AM	Aruba AA
Ashmore and Cartier Islands AT	Australia AS
Austria AU	Azerbaijan AJ
Bahamas, The BF	Bahrain BA
Baker Island FQ	Bangladesh BG
Barbados BB	Bassas Da India BS
Belarus BO	Belgium BE
Belize BH	Benin BN
Bermuda BD	Bhutan BT
Bolivia BL	Bosnia and Herzegovina BO
Botswana BC	Bouvet Island BV
Brazil BR	British Indian Ocean Territory IO
British Virgin Islands VI	Brunei BX
Bulgaria BU	Burkina UV
Burma BM	Burundi BY
Cambodia CB	Cameroon CM
Canada CA	Cape Verde CV
Cayman Islands Republic CT	Central African CJ Chad CD
Chile CI	China CH
Christmas Island KT	Clipperton Islands IP
Cocos (Keeling) Islands CK	Colombia CO
Comoros CN	Cook Islands CW

Coral Sea Islands CR
Cote Devoire IV
Cuba CU
Czech Republic EZ
Djibouti DJ
Dominican Republic DR
Egypt EG
Equatorial Guinea EK
Estonia EN
Europa Island EU
Faroe Islands FO
Fiji FJ
Finland FI
France FR
French Polynesia FP
Gabon GB
Gambia, The GA
Georgia GG
Ghana GH
Glorioiso Islands GO
Greenland GL
Guadeloupe GP
Guatemala GT
Guinea GV
Guyana GY
Heard Island and
  McDonald Islands HM
Hong Kong HK
Hungary HU
India IN
Iran IR
Ireland EI
Italy IT
Jamaica JM
Japan JA
Jersey JE
Jordan JO
Kazakhstan KZ
Kingman Reef KQ
Korea, Democratic
  Peoples Republic KN
Kuwait KU
Laos LA
Lebanon LE
Liberia LI
Liechtenstein LS

Costa Rica CS
Croatia HR
Cyprus CY
Denmark DA
Dominica DO
Ecuador EC
El Salvador ES
Eritrea ER
Ethiopia ET
Falkland Islands
  (Islas Malvinas) FK
Federated States
  of Micronesia FM
French Guiana FG
French Southern and
Antarctic Lands FS
Gaza Strip GZ
Germany GM
Gibraltar GI
Greece GR
Grenada GJ
Guam GQ
Guernsey GK
Guinea-Bissau PU
Haiti HA

Honduras HO
Howland Island HQ
Iceland IC
Indonesia ID
Iraq IZ
Israel IS
Ivory Coast IV
Jan Mayen JN
Jarvis Island DQ
Johnston Atoll JQ
Juan De Nova Island JU
Kenya KE
Kiribati KR

Korea, Republic of KS
Kyrgyzstan KG
Latvia LG
Lesotho LT
Libya LY
Lithuania LH

Luxembourg LU   Macau MC
Macedonia MK   Madagascar MA
Malawi MI   Malaysia MY
Maldives MV   Mali ML
Malta MT   Man, Isle of IM
Marshall Islands RM   Martinique MB
Mauritania MR   Mauritius MP
Mayotte MF   Mexico MX
Midway Islands MQ   Moldova MD
Monaco MN   Mongolia MG
Montenegro MW   Montserrat MH
Morocco MO   Mozambique MZ
Namibia WA   Nauru NR
Navassa Island BQ   Nepal NP
Netherlands NL   Netherlands Antilles NA
New Caledonia NC   New Zealand NZ
Nicaragua NU   Niger NG
Nigeria NI   Niue NE
Norfolk Island NF   Northern Mariana
Norway NO   Islands CQ
Oman MU   Pakistan PK
Palmyra Atoll LQ   Panama PM
Papua New Guinea PP   Paracel Islands PF
Paraguay PA   Peru PE
Philippines RP   Pitcairn Islands PC
Poland PL   Portugal PO
Puerto Rico RQ   Qatar QA
Reunion RE   Romania RO
Russia RS   Rwanda RW
St. Kitts and Nevis SC   St. Helena SH
St. Lucia ST   St. Pierre and
                                     Miquelon SB

St. Vincent and
   the Grenadines VC   San Marino SM
Sao Tome and
   Principe TP   Saudi Arabia SA
Senegal SG   Serbia SR
Seychelles SE   Sierra Leone SL
Singapore SN   Slovakia LO
Slovenia SI   Solomon Islands BP
Somalia SO   South Africa SF
South Georgia and
   the South Sandwich Islands SX Spain SP
Spratly Islands PG   Sri Lanka CE
Sudan SU   Surinam NS
Svalbard SV   Swaziland WZ

Sweden SW	Switzerland SZ
Syria SY	Taiwan TW
Tajikstan TI	Tanzania TZ
Thailand TH	Togo TO
Tokelau TL	Tonga TN
Trinidad and Tobago TD	Tromelin Island TE
Trust Territory of the Pacific Islands (Palau) PS	Tunisia TS
Turkey TU	Turkmenistan TX
Turks and Caicos Islands TK	Tuvalu TV
Uganda UG	Ukraine UP
United Arab Emirates TC	United Kingdom UK
United States US	Uruguay UY
Uzbekistan UZ	Vanuatu NH
Vatican City VT	Venezuela VE
Vietnam VM	Virgin Islands VQ
Wake Island WQ	Wallis and Futuna WF
West Bank WE	Western Sahara WI
Western Samoa WS	Yemen (Aden) YM
Zambia ZA	Zimbabwe ZI

Block 9. Date of Birth. Enter the employee's date of birth in four-digit year, three alphacharacter month, and two-digit day format (YYYYMMMDD). Date of birth must also be entered, when using "U" code (block 12.) for off-line entry. (Use nine characters.)

Block 10. Place of Birth. Enter the employee's place of birth (City, State, and Country, if outside United States). Use State abbreviations provided below. If place of birth is a foreign country, use abbreviation from block 8.

Alabama AL	Pacific AP
Alaska AK	American Samoa AS
Arizona AZ	Arkansas AR
California CA	Colorado CO
Connecticut CT	Delaware DE
District of Columbia DC	Florida FL
Georgia GA	Guam GU
Hawaii HI	Idaho ID
Illinois IL	Indiana IN
Iowa IA	Kansas KS
Kentucky KY	Louisiana LA
Maine ME	Maryland MD
Massachusetts MA	Michigan MI
Minnesota MN	Mississippi MS
Missouri MO	Montana MT

Nebraska NE	Nevada NV
New Hampshire NH	New Jersey NJ
New Mexico NM	New York NY
North Carolina NC	North Dakota ND
Ohio OH	Oklahoma OK
Oregon OR	Pennsylvania PA
Puerto Rico PR	Rhode Island RI
South and Central AA	
America	South Carolina SC
South Dakota SD	Tennessee TN
Federated States	
of Marshall Islands,	
Palau TT	Texas TX
Utah UT	Vermont VT
Virginia VA	Virgin Islands VI
Washington WA	West Virginia WV
Wisconsin WI	Wyoming WY

Block 11. Last Update. Leave blank, no action required. This date is generated automatically by the DEERS and indicates the date of the last online transaction or DD Form 1172-2 submitted for that employee.

Block 12. V/I (Verify and/or Issue). Enter the correct action abbreviation to show the reason that the DD Form 1172-2 is being prepared. Select from the valid values listed in the left column, below. (Use one character.)

A - To indicate the addition of a new record on the DEERS.
C - To indicate a change or update transaction, when an ID card shall not beissued.
I* - To indicate the issue OR reissue of an ID card.
U - To indicate an employee address update only.
T - Terminate
* With initial enrollment and immediate issue of ID card, use "I".

Block 13. Current Residence Address. Enter the number and street of the employee's current residence address. (Use no more than 27 characters.)

Block 14. Supplemental Address Information. Enter supplemental address information, such as an apartment number. Do not enter a duty address in combination with a residence address. This field may be left blank. (Use no more than 20 characters.)

Block 15. City. Enter the employee's current city of residence. If the employee's address is an Army Post Office (APO) or a Fleet Post Office (FPO), enter the designation APO or FPO. (Use no more than 18 characters.)

Block 16. State. Enter the correct U.S. postal abbreviation for the State of the employee's

residence from the valid abbreviations listed, below. If the employee's address is an APO or FPO, enter the correct APO or FPO State. If the employee lives outside of the 50 United States, the District of Columbia, or one of the listed trust territories, enter a default value of "XX." (Use two characters.)

Europe & Canada AE	Alabama AL
Pacific AP	Alaska AK
American Samoa AS	Arizona AZ
Arkansas AR	California CA
Colorado CO	Connecticut CT
Delaware DE	District of Columbia DC
Florida FL	Georgia GA
Guam GU	Hawaii HI
Idaho ID	Illinois IL
Indiana IN	Iowa IA
Kansas KS	Kentucky KY
Louisiana LA	Maine ME
Maryland MD	Massachusetts MA
Michigan MI	Minnesota MN
Mississippi MS	Missouri MO
Montana MT	Nebraska NE
Nevada NV	New Hampshire NH
New Jersey NJ	New Mexico NM
New York NY	North Carolina NC
North Dakota ND	Ohio OH
Oklahoma OK	Oregon OR
Pennsylvania PA	Puerto Rico PR
Rhode Island RI	
South and Central AA America	South Carolina SC
South Dakota SD	Tennessee TN
Federated States of Marshall Islands, Palau TT	Texas TX
Utah UT	Vermont VT
Virginia VA	Virgin Islands VI
Washington WA	West Virginia WV
Wisconsin WI	Wyoming WY

Block 17. ZIP Code. Enter the correct nine-digit ZIP Code of the employee's current residence address in the following format: "123456789." If the last four digits are unknown, enter four zeros (0000); e.g., "123450000." If the employee does not reside in one of the 50 United States, the District of Columbia, or one of the listed trust territories, enter the applicable foreign ZIP Code, or APO or FPO number. If ZIP Code is unknown, leave blank. (Use no more than nine characters.)

Block 18. Country. Enter the employee's correct country of residence from the valid

abbreviations listed in the instructions for Block 8. If the employee's address is an APO or FPO, the country must be "US". If country is unknown, leave blank. (Use two characters.)

Block 19. Home E-mail Address. Enter the employee's home e-mail address, if applicable. If the employee does not have an e-mail account at home, leave this block blank.

Block 20. City of Duty Location. Enter the city of the employee's duty location.

Block 21. State of Duty Location. Enter the correct U.S. postal abbreviation for the State of the employee's duty location from the valid abbreviations listed in the instructions for Block 16. If the employee's address is an APO or FPO, enter the correct APO or FPO State. If the employee works outside of the 50 United States, the District of Columbia, or one of the listed trust territories, enter a default value of "XX." (Use two characters.)

Block 22. Country of Duty Location. Enter the employee's correct country of duty location from the valid abbreviations listed in the instructions for Block 8. If country is not listed, leave blank. (Use two characters.)

Block 23. Office E-mail Address. Enter the employee's office e-mail address as applicable. If the employee does not have an e-mail account, leave this block blank.

Block 24. Sponsoring Office Name. Enter the name of the organization the employee works for or is assigned to for contract purposes.

Block 25. Contract Number. Contract number under which contractor employee is providing support to the Department of Defense.

Block 26. Sponsoring Office Address. Enter the number and street, city, state, zip code, and country code (see Block 8 for country codes) of the employee's sponsoring office address.

Block 27. Sponsoring Office Telephone Number. Enter the employee's sponsoring office telephone number beginning with the area code. Do not use punctuation to separate area code, prefix, and basic number. (Use no more than 14 characters.)

Block 28. Supplemental Address Information. Enter supplemental address information, such as suite number, room number, stop number, and installation name. This field may be left blank.

Block 29. Overseas Assignment. Enter Y (yes) or N (no) as applicable, and the employee's country of assignment from the valid list of abbreviations in the instructions for Block 8. If country is not listed, leave blank.

Block 30. Overseas Assignment Begin Date. Enter the appropriate employee's effective begin date four-digit year, three alpha-character month, and two-digit day format

(YYYYMMMDD) for their overseas assignment. Obtain this information from the employee's personnel documents authorizing their employment overseas.
Block 31. Overseas Assignment End Date. Enter the appropriate employee's effective end date four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD) of their overseas assignment. The period of employment may be obtained from the employee's orders authorizing their employment overseas.

Block 32. Type Of Card Issued. If the transaction being performed results in issue or reissue of the employee's Common Access Card, enter the appropriate abbreviation from the left column, below, to indicate which Form was issued to the sponsor.

    CIV GC - United States DoD/Uniformed Services Geneva Conventions
                   Identification Card for Civilians Accompanying the Armed Forces.
    PRIV   - United States DoD/Uniformed Services Identification and Privilege
                   Card
    CIV   - United States DoD/Uniformed Services Identification Card

Block 33. Elig St/Eff Date. (Eligibility Start Date and/or Effective Date) Enter the date fourdigit year, three alpha-character month, and two-digit day format (YYYYMMMDD) the employee's qualifying status began.

Block 34. Card Expiration Date. Enter the appropriate employee effective end date, not to exceed three years. Use four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD) for the Common Access Card.

    (Note: CACs will be issued for a period of three years, or the individual's term of service, employment or association with the DoD, whichever is earlier. For contractor employees this will normally be the end of the current fiscal year or one year (date of annual contract renewal option.)

Block 35. Supplemental Assignment Information. Enter as applicable any additional assignment information that may be used to identify the organization and location of the employee's assignment.

SECTION II - EMPLOYEE DECLARATION AND REMARKS

Block 36. Remarks. Enter the method of verification and further explanation of qualifying status, such as SF 52, or Contract Number, hiring agency, and period of contract. Indicate other appropriate comments, such as particular work assignment. (That block may contain up to five typed lines of information.)

Block 37. Signature. When the DD Form 1172-2 is not signed in the presence of the verifying official, the signature must be notarized. The notary seal and signature should be placed in the right margin of Block 36., above. Block must contain the employee's signature, with the following exception: (Signature is required.)

When the DD Form 1172-2 is prepared for terminating eligibility and the verifying official has viewed the appropriate documentation, the verifying official may sign.

Block 38. Date Signed (YYYYMMMDD). Enter the date four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD) that block 37 was signed on the DD Form 1172-2.

SECTION III – AUTHORIZED/VERIFIED BY

Officials designated to authorize or verify the DD Form 1172-2 are responsible for the accuracy of the data on the form and must substantiate the data through appropriate documentation, e.g., birth certificates or passports establishing citizenship.

Block 39. Type Name (Last, First, Middle). Enter the information pertaining to the authorizing or verifying official. (Use no more than 51 characters.)

Block 40. SSN. Enter the Social Security Number of the authorizing official.

Block 41. Unit/Organization Name. Enter the unit and/or command name for the verifying official. (Use no more than 26 characters.)

Block 42. Title. Enter the authorizing/verifying official's title. (Use no more than 24 characters.)

Block 43. Pay Grade. Enter the pay grade of the authorizing/verifying official. (Use no more than four characters.)

Block 44. Duty Phone Number. Enter the authorizing/verifying official's duty telephone number. (Use no more than 14 characters.)

Block 45. Unit and/or Organization Address (Street, City, State, and ZIP Code). Enter the mailing address for the verifying official. (Use no more than 28 characters.)

Block 46. Signature. The authorizing/verifying official must sign in that block. (That block must contain the verifying official's signature.)

Block 47. Date Verified (YYYYMMMDD). Enter the date four-digit year, three alphacharacter month, and two-digit day format (YYYYMMMDD) of verification. (Use nine characters.)

SECTION IV - ISSUED BY

Blocks 48. through 56. Enter in the same manner as the verifying official, as prescribed in section III, above.

SECTION V - RECIPIENT'S ACKNOWLEDGMENT

Block 57. Recipient's Signature. Recipient must sign in that block. If the recipient is incapable of signing, the condition must be indicated in that block.
Block 58. Date Signed (YYYYMMMDD). Enter the date four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD) of recipient' s acknowledgment. (Use nine characters.)

13 Appendix C: Schedule for e-mail Contractor reverification notifications

Reverification Required – First Notification – First transmitted 150 days after application approved

Dear {TA},

This message has been sent to notify you that you need to reverify the contractor ({Contractor}) requires his/her CAC. Please complete the verification process at the link below.

Questions may be sent via email to: cvs.helpdesk@osd.pentagon.mil

CVS TA Web Site: https://www.dmdc.osd.mil/appj/cvs/taLogin.jsp

Reverification Timeout Warning 1 – First transmitted 15 days after first notification

Dear {TA},

This message has been sent to remind you the prescribed time to reverify contractor ({Contractor}) has arrived. Please complete the verification process as prescribed.

Questions may be sent via email to: cvs.helpdesk@osd.pentagon.mil

CVS TA Web Site: https://www.dmdc.osd.mil/appj/cvs/taLogin.jsp

Reverification Timeout Warning 2 – First transmitted 30 days after first notification

Dear {TA},

This message has been sent to notify you the prescribed time to reverify contractor ({Contractor}) has arrived and that that action needs immediate attention. Please complete the verification process as prescribed. The time allotted for you to complete the verification will expire on {Date} at which time the contractor's Defense Enrollment Eligibility Reporting Service record will be terminated.

Questions may be sent via email to: cvs.helpdesk@osd.pentagon.mil

CVS TA Web Site: https://www.dmdc.osd.mil/appj/cvs/taLogin.jsp

---

Reverification Timeout – Transmitted 45 days after first notification

Dear {TA},

The time allotted to reverify contractor {Contractor} has expired. As a result, that account has been revoked and the Defense Enrollment Eligibility Reporting System has been updated to reflect the change.

Questions may be sent via email to: cvs.helpdesk@osd.pentagon.mil

CVS Web Site: https://www.dmdc.osd.mil/appj/cvs/

14 Appendix D: Acronyms, Abbreviations, and Terms

ACO	Access Card Office
C&A	Certification and Accreditation
CA	Certificate Authority
CAC	Common Access Card
CT&IS	Card Technology and Identity Solutions
ConOps	Concept of Operations
CVS	Contractor Verification System
DISA	Defense Information Systems Agency

DEERS	Defense Enrollment & Eligibility Reporting System
DMDC	Defense Manpower Data Center
DoD	Department of Defense
EBUSOPSOFF	eBusiness Operations Office (Navy)
EDI-PI	Electronic Data Interchange Person Identifier
EEPROM	Electronically Erasable Programmable Read Only Memory
EJB	Enterprise Java Bean
FAQ	Frequently Asked Question
Government Sponsor	Active Duty member or Civil Servant who approves contractor CAC request
ICC	Integrated Circuit Chip
ID	Identification
J2EE	Java v.2 Enterprise Edition
JSP	Java Server Page
LMS	Learning Management System
NMCI	Navy Marine Corps Intranet
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point of Contact
RAPIDS	Real-time Automated Personnel Identification System
SSL	Secure Socket Layer
SSM	Site Security Manager (RAPIDS)
SSN	Social Security Number
TA	Trusted Agent
TASM	Trusted Agent Security Manager
VO	Verifying Official (RAPIDS)